COMPUTING THE IMPACT OF SECURITY ATTACK ON NETWORK USING FUZZY LOGIC

Mohammad Mudassar[1], Prof. A.P.Kankale[2], Prof. P.S.Gawande[3]

[1]*PG Scholar, Dept. Of CSE, Rajarshi Shahu College of Engineering, Buldhana [M.S] India.*
[2]*Head of Dept. (CSE) Rajarshi Shahu College of Engineering, Buldhana [M.S] India.*
[3]*Head of Dept. (EXTC) Rajarshi Shahu College of Engineering, Buldhana [M.S] India.*

---***---

Abstract - *Security of computer and networking systems have been an issue since computer networks became widespread. Cyber threat puts serious threats to the integrity, confidentiality and availability of data for the whole internet and intranet users. Cyber security and intrusion detection has emerged as a significant field of research, because it is not theoretically possible to set up a complete system with no fault. Intrusion incidents to computer systems are increasing because of the widespread usage of the internet and local networks. It is known that different machine learning algorithms, for example support vector machine, genetic algorithm, neural network , data mining, fuzzy logic and some others have been extensively applied to detect intrusion activities.*

This paper presents an efficient method of computing the influence of security attack on network using fuzzy logic.

Key Words: **Mudassar, fuzzy logic, security attack, intrusion detection, network security.**

1.INTRODUCTION

A wireless network allows the people access application and information without wires. This provides the facilities to access application different parts of the building, city, or anywhere in the world. Wireless network allows people to communicate with e-mail or browse from a location that they prefer [3]. A wireless sensor network is a wireless network consisting of distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as sound, vibration, pressure, at different locations. The development of wireless sensor networks motivated by military such as battlefield surveillance, however, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications. A wireless sensor network is a collection of nodes organized into a cooperative network each node consists of processing capability may contain multiple types of memory have an RF transceiver, have a power source e.g., batteries. The wireless network consists of thousands of low-power, low-cost nodes deployed to monitor and affect the environment [7]. Wireless sensor network emerged as mean study to interact with physical world. The wireless sensor technology has made it possible to deploy small, low-power, low-bandwidth and multifunctional wireless sensor nodes to monitor and report the conditions and events in different challenging environment [11]. A wireless sensor becomes a very popular because wireless nodes monitor and report the different environments. Wireless sensor network rapidly used in military, wildlife monitoring, earthquake monitoring, building safety. Wireless sensor network have recently emerged an important means study and interact with physical world. The recently technological advances in wireless sensor technology has made it possible to deploy small, low-power, low bandwidth, and multifunctional wireless sensor nodes to monitor and report the conditions and events in different challenging environment. As wireless sensor network continue to grow there is need for effective security mechanisms. Because sensor network may interact with sensitive data or operate in unattended environment it is necessary that these security concerns should be addressed from the beginning of the system design [9]. However, security in sensor network poses different challenges for network security. Thus design mechanism of security very critical of the better and wider adaptability of this network in commercial scenarios. This paper investigates various security attacks on wireless sensor network and their impact on WSN

1.1 Fuzzy Logic

The fuzzy set theory was introduced by Zadeh. Fuzzy logic is a multi-value logic which permits intermediate values to be defined between conventional ones like true/false, low/high, good/bad etc. In a classical set theory, an element may either belong to set or not. In fuzzy set theory, an element has a degree of membership. A degree of membership function can be described as an interval [0, 1]. A fuzzy expert system is simply an expert system that uses a variety of fuzzy membership functions and rules, instead of Boolean logic, to reason about data. The rules in a fuzzy expert system are usually in a form of the following:

- If A is low and B is high then X= medium where A and B are input variables, X is an output variable.

Forward Chaining: An expert system rule may be formulated simply as “if A then B” where A is a set of conditions on data and B is a set of instructions to be carried out when the rule is fires. The rules are examined to see which rules are made firable by the data, that is, A is satisfied, and a rule or rules selected for executing. When the rule is executed, the set of instructions B is executed. Most rule-based expert systems works in this way . Forward chaining is used in proposed model.

Backward chaining: A different sequence is followed in backward chaining. In backward chaining, we specify what conclusion we would like to reach, that is, we specify B. We find a rule or rules that have the desired consequent, and look at the antecedent A to see what the data must be to satisfy A. Now we find out how those data can be established, and look for rules that have those data as a consequent, or input data from a user to see if the antecedent can be satisfied. In backward chaining we work backward from goals to data; in forward chaining we work forward from data to goals

In this paper, the expert system roles have been designed to capture the details of cyberattacks. After that the system can use them and offer recommendations for system administrator.

2. LITERATURE SURVEY

To minimize the chances of software project failure need to proper study all the risk factors which can have direct or indirect effect on the success of software product. Much application development used to make the software in efficient manner and various steps each risk defined. Tools are available for management of various kinds of risks. Fuzzy logic approach used to identify threats for the risks [3] [10]. This logic is composed of fuzzy sets, provides the concept of degrees of membership, which increases the number of possibilities that can be subject to research. This logic is perfect deal with uncertain risk come in project management [6].

2.1 Types of Attacks on Network

- *Jamming attack*- Jamming attacks launched at MAC layer.
- *Clone attack* – In this attack the attacker replicate the nodes in the form of clone.
- *Route information manipulation attack* - In this attack the attacker gives a false routing information.
- *Denial of service attack* – It is occurred by the failure of node or malicious action.
- *Eavesdropping attack* - Adversary listen message transmitted to nodes.
- *Collision attack* – It creates Interruption in the working wireless sensor network.
- *Sink hole attack* – In a sinkhole attack is a serious threat in it compromised node tries to all or much traffic possible from a particular area.
- *Traffic analysis attack*- It is a type of security attack which create a traffic on a wireless sensor network.
- *De- synchronization attack* – De- synchronization changes sequences number of packet.
- *Selective forwarding attack* – In this attack compromised node drops packets which effect on network efficiency.

3. Designing an expert system using fuzzy logic.

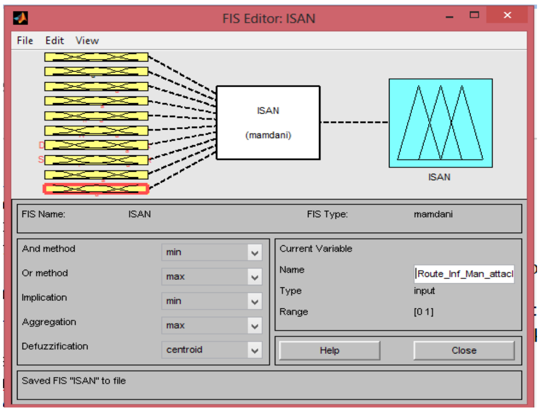
To design our proposed system using fuzzy logic we have to follow these steps-

3.1. Defining Input and Output parameters.

The input variables are determined based on the properties that should be incorporated or eliminated in a system. For example the properties to be incorporated into a secure system are used in this work. These are confidentiality, integrity and availability.
For each of the input, suppose that the domain interval is [0;+s] e.g. [0 ⍰ 10], each of them defined individually.
The domain is divided into 2N + 1 regions and each region is attached a fuzzy membership function. In this work, the domain is divided into 5 regions (N =2). The regions are represented by triangular membership functions.
There will be 10 Input Parameters as follows:

1) Denial of service attack
2) Eavesdropping attack
3) Collision attack
4) Sink hole attack
5) Traffic analysis attack
6) De- synchronization attack
7) Selective forwarding attack
8) Jamming attack
9) Clone attack
10) Route information manipulation attack

There will be single output parameter named ISAN(Impact of Security Attack on Network)



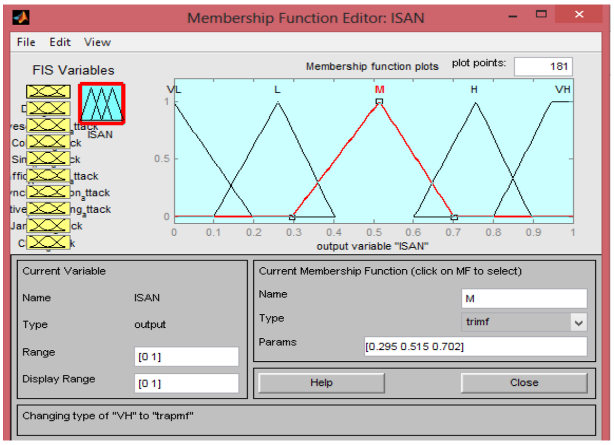
FIS Name: ISAN
FIS Type: mamdani
And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid
Current Variable
Name: Route_Inf_Man_attacl
Type: input
Range: [0 1]
Saved FIS "ISAN" to file

Fig.1- Input & Output parameters.

The fuzzy inference system editor shows a summary of the fuzzy inference system. It shows the mapping of the inputs to the system type and to the output. The names of the input variables and the processing methods for the FIS can be changed through the FIS editor.

3.2. Defining membership functions for output parameter ISAN

There will be 5 membership functions of ISAN in order to describe the level of impact of attack on network very low, low, medium, high, very high.



plot points: 181

Current Variable
Name ISAN
Type output
Range [0 1]
Display Range [0 1]

Current Membership Function (click on MF to select)
Name M
Type trimf
Params [0.295 0.515 0.702]

Changing type of "VH" to "trapmf"

Fig. 2-Defining membership functions for ISAN

3.3. Defining Fuzzy Rules for the System

1. If (Denial_ of_ service is Yes) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is No) and (jamming_ attack is Yes) and (clone_ attack is No) and (Route information_ manipulation is Yes) and (Selective_ forwarding is No) then (ISAN is H)

2. If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is No) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is No) and (Route information_ manipulation is Yes) and (Selective_ forwarding is Yes) then (ISAN is VH)

3. If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is Yes) and (De-synchronization is Yes) and (collision is Yes) and (Sink_ hole is No) and (jamming_ attack is No) and (clone_ attack is No) and (Route_ information_ manipulation is No) and (Selective_ forwarding is No) then (ISAN is M)

4. If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is Yes) and (De- synchronization is Yes) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is Yes) and (Route_ information_ manipulation is Yes) and (Selective_ far warding is Yes) then (ISAN is VH)

5. If (Denial_ of_ service is No) and (Eavesdropping is Yes) and (Traffic_ analysis is No) and (De- synchronization is No) and (collision is No) and (Sink_ hole is No) and (jamming_ attack is No) and (clone_ attack is No) and (Route_ information_ manipulation is No) and (Selective_ far warding is No) then (ISAN is VL)

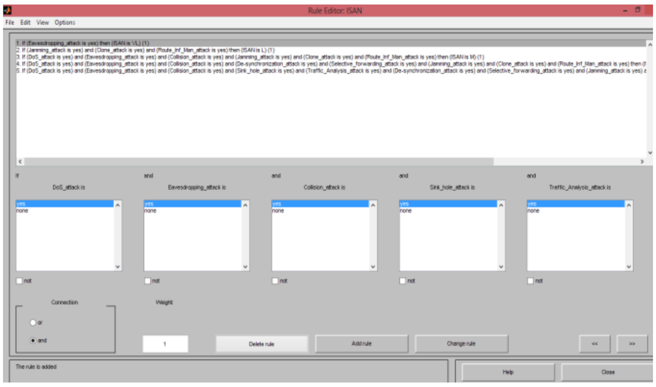
6. If (Denial_ of_ service is Yes) and (Eavesdropping is No) and (Traffic_ analysis is No) and (De- synchronization is No) and (collision is Yes) and (Sink_ hole is No) and (jamming_ attack is No) and (clone_ attack is No) and (Route_ information_ manipulation is No) and (Selective_ far warding is No) then (ISAN is L)

7. If (Denial_ of_ service is No) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is No) and (Sink_ hole is Yes) and (jamming_ attack is Yes) and (clone_ attack is Yes) and (Route information_ manipulation is Yes) and (Selective_ forwarding is No) then (ISAN is H)

8. If (Denial_ of_ service is Yes) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is Yes) and (clone_ attack is Yes) and (Route information_ manipulation is Yes) and (Selective_ forwarding is Yes) then (ISAN is VH)

9. If (Denial_ of_ service is Yes) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is No) and (Route information_ manipulation is Yes) and (Selective_ forwarding is No) then (ISAN is M)

10. If (Denial_ of_ service is No) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is No) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is No) and (Route information_ manipulation is No) and (Selective_ forwarding is No) then (ISAN is VL)


1. If (Eavesdropping_attack is yes) then (ISAN is VL) (1)
2. If (Jamming_attack is yes) and (Clone_attack is yes) and (Route_Inf_Man_attack is yes) then (ISAN is L) (1)
3. If (DoS_attack is yes) and (Eavesdropping_attack is yes) and (Collision_attack is yes) and (Jamming_attack is yes) and (Clone_attack is yes) and (Route_Inf_Man_attack is yes) then (ISAN is M) (1)
4. If (DoS_attack is yes) and (Eavesdropping_attack is yes) and (Collision_attack is yes) and (De-synchronization_attack is yes) and (Selective_forwarding_attack is yes) and (Jamming_attack is yes) and (Clone_attack is yes) and (Route_Inf_Man_attack is yes) then (
5. If (DoS_attack is yes) and (Eavesdropping_attack is yes) and (Collision_attack is yes) and (Sink_hole_attack is yes) and (Traffic_Analysis_attack is yes) and (De-synchronization_attack is yes) and (Selective_forwarding_attack is yes) and (Jamming_attack is yes) a

The rule is added

Fig.3-Rule Editor .

This rule based system help to analysis risks on WSN and provides ability to see the Security attack which provides highly influences on the WSN. We constructed 40 rule base systems with different rules take guidance form including the WSN Organizations, Network, Manager, and Network companies. The impact of Security attack upon WSN, The impact levels of the risks are categorized into five levels. The impact Attack is categorized into five levels. The impact of risk can be "very low", "Low", "Medium", "High", very high". The inputs are represented by fuzzy system. Membership function is used to represent the fuzzy sets. Membership function of the system are as shown in fig 2.Membership function (MF) is a curve that defines how each point in the input is mapped to a membership value (or degree of membership) between 0 and 1.The membership functions are formed using straight lines of these, the simplest is the triangular membership function, and it has the function name trimf is a collection of three points forming a triangle. The trapezoidal membership function, trapmf, consists of truncated triangle curve. The membership function igbellmf (generalized bell membership function) and Gaussian membership function gaussmf define the fuzzy sets. Polynomial based curves account for several of the membership functions in the toolbox. Three related membership functions are the Z, S, and Pi curves, all named because of their shape. The function zmf is the asymmetrical polynomial curve open to the left, it defined Z- shape. Smf is the mirror-image function that opens to the right, and defines the S-shape. pimf is zero on both extremes with a rise in the middle. Fig 1 shows the input output parameters. Rule editor given in figure 3 change and delete the rule. Rule editor helps to add and delete the rules. In the rule editor rule are formulated after representing input and output of fuzzy sets in membership functions.

4. RESULTS & DISCUSSIONS

Rule based Technique is the type of tool that helps to detect the Security attack influence on WSN. It is used for the different decision making. Rule based system presents information graphically and may include an expert knowledge. It is a specific class of computerized system that supports business and organization and decision activates. A Rule based system is an software based system intended to help decision maker compile the useful information from raw data, documents personal knowledge and business model to solve the problem.

The system for calculating the impact of security attack on network was successfully designed and developed. The fuzzy logic toolbox of Matlab was used.
The experimental results were as follows:

Case 1: The following output shows that out of 10, when 8 attacks were made on the network , the impact was near about 0.567 i.e there was a 'high' effect on the system by the attack.

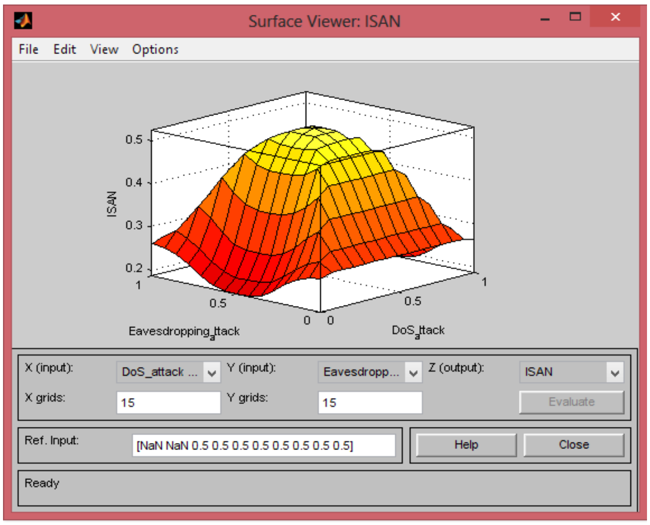

X (input): DoS_attack
Y (input): Eavesdropping_attack
Z (output): ISAN
X grids: 15
Y grids: 15
Ref. Input: [NaN NaN 0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5]
Ready

Fig.4- Sample Output 1

Case 2: This is another sample where output parameter ISAN is shown corresponding to De-synchronization & Sink-hole attack.

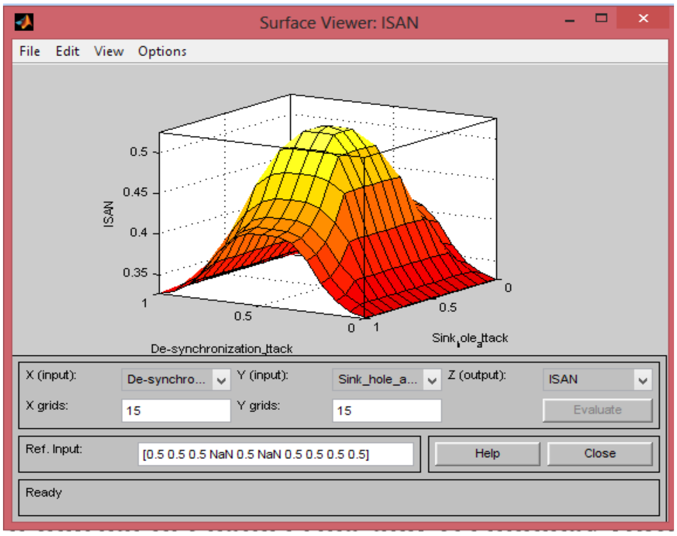

X (input): De-synchronization_attack
Y (input): Sink_hole_attack
Z (output): ISAN
X grids: 15
Y grids: 15
Ref. Input: [0.5 0.5 0.5 NaN 0.5 NaN 0.5 0.5 0.5 0.5]
Ready

Fig.5- Sample Output 2.

Many such outputs can be obtained by giving different inputs.
Fuzzy logic approach had been known as powerful tool for risk assessment due to the fact that most approaches from classical statistics assume that they deal with exact measurements. But in most, if not all real scenarios, there is no precise measurements. Based on that fact, in this paper new method for assessing cyber security risk is introduced.

The proposed method is based on a new risk model which takes into account many risk factors such as system vulnerabilities, the likelihood of exploiting such vulnerabilities, and the likelihood of success. Also, the characteristics of a threat source such as his capabilities, intent, and targeting. The principal advantage of this method is the realistic modeling to systems environment in contrast to the common risk model which takes only into account the likelihood of an event and the impact of that event.

5. CONCLUSION

Many method of the fuzzy rule based system has been applied and different case study has been presented in this paper discussed various kinds of security attack and their impact on WSN. As the wireless sensor continue to grow and become more common there is strong requirement to secure these networks for better and wider adaptability in commercial scenario. A secure WSN design consists of proper attack detection and design mitigation techniques.

The result of this study shows that if the software producing companies will incorporate security risk analysis into the production of software system, the issue of insecurity of software will be held to the minimum if not eliminated. This study has also revealed that if each of the software security goals can be increased to the maximum, then the level security will also be increased and the risk associated will be eliminated.

Finally, security risk analysis is a path towards producing secure software and should be considered a significant activity by software development organisations.

This study proposes a fuzzy rule based cyber indicator that warns system administrators for expected cyber threats. It has been found that a system works well when applied with a given cyber threat scenario (please see the simulation results). This facilitates some warning signals generated by the rules. The model's goal is not to protect a system; however it aims at warning the system administrator for expected cyber threats. The proposed model shows its superiority in the areas of development flexibility and fast response for cyber threats. The model can be used by system administrators in order to determine the nature of cyber threat triggered by cyber terrorists. Also, it can be used by commercial firms or government institutions to form a more secured knowledge environment.

It could be attractive to the researchers to compare the performance of fuzzy rule based expert system with other meta-heuristics (e.g. Artificial Neural Network, Genetic Algorithm, Fuzzy Neural Networks) or regular statistical methods (Linear/Nonlinear Regression). A special interest would be on testing whether fuzzy rule based approach has any advantage in dealing with the cyber security threats.

6. FUTURE WORK

It might be necessary to redesign this system in a way that it will be deployable and will be without the use of MATLAB. It might also be necessary to use an adaptive fuzzy logic technique for security risk analysis. We have been able to design a system that can be used to evaluate the security risk associated with the production of secure software systems. This will definitely help software organizations meet up with the standard requirements. A technique for assessing security of software system before final deployment has been presented.

7. REFERENCES

[1]. Mohit Malik, Namarta kapoor, Esh naryan, Aman Preet Singh "Rule Based Technique Detecting Security Attack for WSN using Fuzzy Logic." International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012

[2]. Abdel-Azim, M.; Abdel-Fatah, A.I.; Awad, M.; "Performance analysis of artificial neural network intrusion detection systems," Electrical and Electronics Engineering, 2009. ELECO 2009. International Conference on , vol., no., pp.II-385-II-389, 5-8 Nov. 2009

[3]. Peng Shanguo; Wang Xiwu; Zhong Qigen; , "The study of EM algorithm based on forward sampling," Electronics, Communications and Control (ICECC), 2011 International Conference on , vol., no., pp.4597-4600, 9-11 Sept. 2011 doi: 10.1109/ICECC.2011.6067693

[4]. Fisher, D.; Ling Xu; Carnes, J.R.; Reich, Y.; Fenves, J.; Chen, J.; Shiavi, R.; Biswas, G.; Weinberg, J.; , "Applying AI clustering to engineering tasks," IEEE Expert , vol.8, no.6, pp.51-60, Dec. 1993 doi: 10.1109/64.248353

[5]. J.-S. R. Jang, C.-T. Sun, E.Mizutani, Neuro-Fuzzy and Soft Computing, p (426-427)Prentice Hall, 1997

[6]. Maria Colmenares & Olaf Wolken Hauer, "An Introduction into Fuzzy Clustering", http://www.csc.umist.ac.uk/computing/clustering.htm, July 1998, last update 03 July,2000

[7].http://home.dei.polimi.it/matteucc/Clustering/tutorial_html/cmeans.html

[8]. www.ics.uci.edu/pub/ml-repos/machine-learning-database/, 2001

[9]. Von Altrock, Constantin (1995). Fuzzy logic and Nero Fuzzy applications explained. Upper Saddle River, NJ: Prentice Hall PTR. ISBN 0-13-368465-2

[10]. Arabacioglu, B. C. (2010). "Using fuzzy inference system for architectural space analysis" Applied Soft Computing 10 (3): 926–937. DOI:10.1016/j.asoc.2009.10.011.

[11]. Biacino, L.; Gerla, G. (2002). "Fuzzy logic, continuity and effectiveness" Archive for Mathematical Logic 41 (7): 643–667. DOI:10. 1007/s001530100128. ISSN 0933-5846

[12]. Cox, Earl (1994). The fuzzy systems handbook: a practitioner's guide to building, using, maintaining fuzzy systems. Boston: AP Professional. ISBN 0-12-194270-8

[13]. Ozyilmaz, L.; Yildirim, T.; "Diagnosis of thyroid disease using artificial neural network methods," Neural Information Processing, 2002. ICONIP '02. Proceedings of the 9th International Conference on , vol.4, no., pp. 2033- 2036 vol.4, 18-22 Nov. 2002 doi: 10.1109/ICONIP.2002.1199031

BIOGRAPHIES

Mr.Mohammad Mudassar
The author was born on 1 Sept, 1991.
He completed his bachelor’s degree in Information Technology in 2013 from the Rajarshi Shahu College of Engineering, Buldhana & is presently pursuing his master’s degree in Computer Science & Engg. He started research work from the year 2013. His main area of interest is fuzzy logic, cyber security & expert systems. He has successfully published 2 research papers in IJPRET in 3rd & 4th International Conferences on Emerging Trends & Research in Engineering & Technology held at IBSS Amravati[M.S] India. This paper is his next contribution in the field of research studies.