INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DESIGNING FORWARD CHAINING INFERENCE ENGINE FOR FUZZY RULE BASED EXPERT SYSTEM FOR CYBER SECURITY

MOHAMMAD MUDASSAR[1], PROF. A. P. KANKALE[2]

1. PG Scholar. Department Of Computer Science & Engg. Rajarshi Shahu College of Engineering, Buldhana.
2. Head Of Department (Computer Science & Engg.) Rajarshi Shahu College of Engineering, Buldhana.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Critical infrastructure sites and facilities are becoming increasingly dependent on interconnected physical and cyber based real time distributed control systems. A mounting cyber security threat results from the nature of these ubiquitous and sometimes unrestrained communications interconnections. Cyber security is not a single problem, but rather it is a group of highly different problems involving different sets of threats. A Cyber Security System using fuzzy logic is a system that consists of a rule depository and a mechanism for accessing and running the rules. Fuzzy optimization deals with finding the values of input parameters of a complex simulated system which results in desired output. Fuzzy logic controller is used to execute fuzzy logic inference rules from a fuzzy rule base in determining the congestion parameters, getting the warning information and the appropriate action. To simulate the situation of an advance cyber security system using fuzzy logic, we use MATLAB. The model's goal is not to protect a system however it aims at warning the system administrator for expected cyber threats. The proposed study shows its superiority in the areas of development flexibility and fast response for cyber threats.

Keywords: Mudassar, Fuzzy Rule Based Expert System For Cyber Security, Fuzzy Logic, Cyber Security, Expert System, Forward Chaining Inference Engine.

Corresponding Author: MR. MOHAMMAD MUDASSAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Mohammad Mudassar, IJPRET, 2016; Volume 4 (9): 725-730

PAPER-QR CODE

INTRODUCTION

Cyber Terrorism

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.

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.

Fuzzy sets and fuzzy number

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.

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

MATERIALS & METHODS

Designing a Fuzzy Rule Based Expert System for Cyber Security

The designing stages include defining cyber security expert system variables, data collection for cyber threats, system design and implementation. These stages are described in the following subsections.

Stage 1: Defining Cyber Security Expert System Variables

The first step in the proposed model is the establishment of input and output variables. This task is usually done by studying the problem domain and by consultation with the cyber experts. There is infinite number of potential candidates which should be restricted to positive numbers. In this paper, the key variables were defined with reference to interviews with cyber security experts. Input and outputs of proposed model is given in following figure.

Input Variables	Abbreviation	Output Variables	Abbreviation
Cyber Techniques	CT	Software	S
Aim of Cyber Intruders	ACI	Hardware	H
Cyber Intruder's Target	CIT	User	U
Cyber Intruders	CI		

Fig 1: Inputs and outputs of proposed model.

Stage 2: Data Collection for Cyber Terrorism

The expert system models the knowledge of the human expert. It also provides explanations similar to the human expert. The system can describe various questions asked by the user. The data used for this work have been extracted from a series of questionnaires collected from cyber experts and system administrators. The obtained data are related especially with topics given below.

- Denial of Service (Dos) attacks, virus, malware, logic bomb, social engineering, Trojan horse,
- Out of service, seizing web page, attacks for protesting, seize critical systems, capture confidential information, system control.

This study evaluates cyber terrorists who might attack communications systems, financial centers, power plants, emergency services, transportation, water supply, oil and natural gas distribution stations. People capable of cyber terrorism such as dedicated special staff, hackers, cyber activists and opponents of the state are evaluated in the proposed model.

Stage 3: System Design

The main modules of a fuzzy rule based system are fuzzification - or fuzzifier module - , fuzzy rules, inference engine and defuzzifier.

1. Fuzzification module: It converts a crisp input of the domain of the input variable domain to a grade by fuzzy set. Constructing a fuzzy logic membership functions play a crucial role for fuzzy rule based models. Triangular membership function was used in many fuzzy logic based applications. In this study triangular membership functions have been used.

2. Defining fuzzy rules: Fuzzy rules consist of antecedent and consequent in the form of IF-THEN statements. There are a number of rules, and they make a group which forms the basis for inference The following some fuzzy rules have been taken with the combination of linguistic variable values.

1. If (CIT is PI) and (CI is SS) then (S is SPS)(H is SC)(U is UT) (1)
2. If (CIT is PI) and (CI is EOS) then (S is SPS)(H is SC)(U is UT) (1)
3. If (CIT is PI) and (CI is CA) then (S is SPS)(H is SC)(U is UT) (1)
4. If (CIT is PI) and (CI is CH) then (S is SPS)(H is SC)(U is UT) (1)
5. If (CT is NA) then (S is SPS) (1)
6. If (CT is DOS) then (H is TS) (1)
7. If (CT is V) then (S is SPS) (1)
8. If (CT is EV) then (S is SPS)(U is A) (1)
9. If (CT is TH) then (S is SPS)(U is A) (1)
10. If (CT is SE) then (U is UT) (1)
11. If (CT is M) then (S is SPS)(U is A) (1)
12. If (CT is LB) then (S is SPS)(U is A) (1)
13. If (ACI is OOS) then (S is SU)(H is TS)(U is UT) (1)
14. If (ACI is SWP) then (H is TS)(U is UC) (1)
15. If (ACI is P) then (H is TS) (1)
16. If (ACI is CCI) then (S is NDB)(H is SC)(U is UC) (1)

3. Defuzzification: It acts as the interface between the fuzzy logic control and the inference system, by providing the crisp output. Regular defuzzification methods are centroid, bisector, mean value of maximum values, smallest value of maximum values and largest value of maximum. The conversion of a fuzzy set to a single crisp value is called defuzzification and reverse process is fuzzification. Mamdani defuzzification method (centroid of the area) is used in the model.

RESULTS & DISCUSSIONS

In Figure of fuzzy rule viewer for the model is shown using MATLAB. According to the proposed model, a sample solution is given in Figure when CT=0.135; ACI=0.32; CIT=0.187; CI=0.57. Here, model outputs are S=0.556; H=0.571 and U=0.861.

Output of S=0.556 means that system needs update (SU); H=0.571 means that system needs special computer (SC); U=0.861 means that user needs user control (UC) is important.

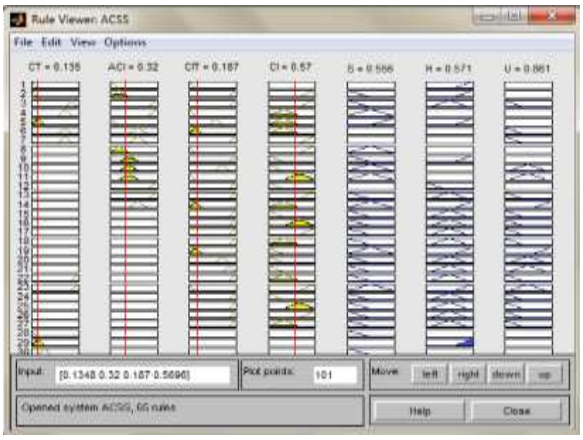

Fig 2: Fuzzy Rule viewer.

SAMPLE SOLUTIONS

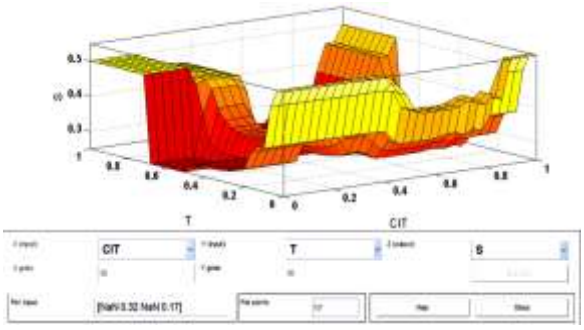

Fig 3: Sample solution set for "CIT-CT- S"

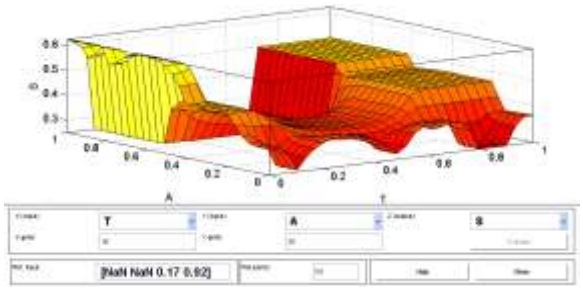

Fig 4: Sample solution set for "CT-CIA-S"

CONCLUSION

In this paper, an expert system for cyber security based on fuzzy rule was presented. After consultation with cyber experts and system administrators, the inputs and output of the system were determined. Mamdani fuzzy inference system was selected. The inference of the fuzzy rules was carried out using the 'min' and 'max' operators for fuzzy intersection and union. A series of fuzzy if-then rules were designed for the knowledge base. Input space was divided into multidimensional partitions in order to formulate the initial rule base. Actions were then assigned to each of the partitions. 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. 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.

REFERENCES

1. Kerim Goztepe, "Designing a fuzzy rule based expert system for cyber security" in International Journal of Information Security Science. Vol 1. No. 1.
2. Javed Alam, Prof. (Dr.) M. K. Pandey, "Advance Cyber Security System using fuzzy logic"
3. Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti, Samir K. Sadhukhan "Cyber-risk decision models: To insure IT or not?" Decision support system of Elsevier May 2013, PP 11-26.
4. Jill Rowland, Mason Rice, Sujeet Shenoi "The anatomy of a cyberpower"