International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 04 (July- August, 2020)

Improved Risk Management Model of Cyber Security Using Advanced Fuzzy Model

Sudhir Sahu, Shital Gupta
Department of CSE, SORT, People's University, Bhopal
[1]Bhopalsudhiresah@gmail.com, [2]email4sgupta@gmail.com

Abstract: *- The topic of cybersecurity has been subject to more attention and interest outside the community of computer security experts. Cybersecurity is not a single problem, but rather it is a group of highly different problems involving different sets of threats. Fuzzy Rule-based system for cybersecurity is a system that consists of a rule depository and a mechanism for accessing and running the rules. The aim of study fuzzy logic is devolved fuzzy logic-based improved risk management model for cybersecurity. The proposed model shows its superiority in the areas of development flexibility and fast response to cyber threats. The model can be used by system administrators to determine the nature of the cyber threat triggered by cyber terrorists. Also, it can be used by commercial firms or government institutions to form a more secured knowledge environment.*

Keywords: - Cyber Security. Scams, firewall, Recognition, Security, Algorithms, Phishing, Cyberspace

1. INTRODUCTION

Cyber-attacks affect every aspect of our lives. These attacks have serious consequences, not only for cyber-security but also for safety, as the cyber and physical worlds are increasingly linked. Providing effective cyber-security requires cooperation and collaboration among all the entities involved. Increasing the amount of cyber threat information (CTI) available for analysis allows better prediction, prevention and mitigation of. [1]Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security. It is important military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that is intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cybersecurity describe the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, needs to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism. The remainder of this work is organized as follows: The scope of this work is presented in the Introduction. In Section 2, we provide a detailed literature review Section 3, we present we mentioned proposed fuzzy methodology Section 4 there is simulation and result and in section 5 there is a conclusion and future work

2. LITERATURE REVIEW

Computer security, and intrusion detection, in particular, has become increasingly important in today's business environment, to ensure safe and trusted commerce between business partners as well as effective organizational functioning. Various approaches to intrusion detection are currently being utilized, but unfortunately, in practice, these approaches are relatively ineffective and inefficient. New means and ways that will minimize these shortcomings must, therefore, continuously be researched and defined. This paper will propose a proactive and dynamic approach, on-trend analysis and fuzzy logic that could be utilized to minimize and control intrusion in an organization's computer system [1]. In the paper, [2] the earlier developed SRFT model has been modified using the concepts of fuzzy logic. In the modified SRFT model, two linguistic fuzzy scales (three-point and four-point) have been devised based on trapezoidal fuzzy numbers. Human subjectivity of different experts associated with previous SRFT model is tackled by mapping their scores to the newly devised fuzzy scale. Finally, the fuzzy score thus obtained is defuzzied to get the results. A test case of a refinery has been taken to compare the results of both the models. The total risk score obtained using the previous SRFT model was '40'. The modified SRFT model gives '38.08'. The final risk score suggests it is a high-risk facility and therefore demands serious security attention. The refinery X should go through detailed security and vulnerability assessment and initiate aggressive risk reduction exercise in coordination with the local law enforcement. Security of computer and networking systems have been an issue since computer networks became widespread. Today the internet is changing social life. Sophisticated computer systems are deployed worldwide in many critical infrastructures ranging from business centres, nuclear power plants, and government agencies to transportation systems.

Cyber threat puts serious threats to the integrity, confidentiality and availability of data for the whole internet and intranet users [3]. Cybersecurity 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 [4]. Intrusion incidents to computer systems are increasing because of the widespread usage of the internet and local networks [5]. It is known that different machine learning algorithms, for example, support vector machine [6], genetic algorithm [7], neural network [8], data mining [9], fuzzy logic [3],[10] and some others have been extensively applied to detect intrusion activities. There are some emerging definitions of cyber terrorism. Terrorism is defined as intentional, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience. The term "international terrorism" means terrorism involving citizens or territory of more than one country. The term "terrorist group" means any group practising, or has significant subgroups that practise, international terrorism [11]. Persistent computer security vulnerabilities may expose the government's critical infrastructure and government's network systems to cyber-attack by terrorists, possibly affecting the economy or other areas of the national security at large [12].

Furnel and Warren [13] discussed the problems posed by cyber terrorists. They considered the nature of the responses necessary to protect the future security of society. By the rising threat of cyber-attacks, some researchers tried to describe the cyber threat and made attempts for finding a solution to their studies [14]-[17]. So far, many studies have been done on cybersecurity, but these are mostly focused on prevention of cyber intrusion, [18]-[21], effects of cyber-attacks or different machine learning applications [5],[6],[8]-[10]. Although some studies are using fuzzy rules [22]-[24], fuzzy expert systems' effectiveness is a different analysis. In this paper, apart from existing literature, a new approach has been developed to prevent cyber-attacks from using a fuzzy expert system. The proposed fuzzy expert system in this study gives valuable information to system administrators to improve the achievement of cybersecurity. This work contributes to the system in a general manner and it can be adapted to different cybersecurity scenarios.

3. FUZZY METHODOLOGY

The existing literature on cybersecurity system has been summarized, and the common limitations in previous works have been highlighted. The designing stages include defining advance cybersecurity system variables, data collection for cyber threats, system design and implementation. These stages are described in the following subsections.

3.1 Structure of Proposed Model

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. There is an infinite number of potential candidates which should be restricted to positive numbers.

3.2 Structure of Proposed Model

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. There is an infinite number of potential candidates which should be restricted to positive numbers.

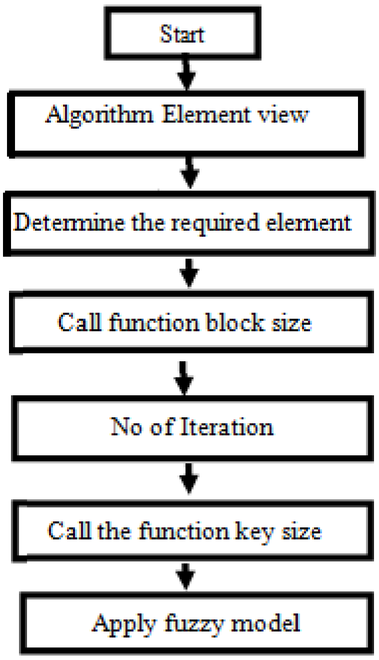


Fig 1: Flow Diagram

In this paper, the key variables are defined. Input and outputs of the proposed model are given in Table 1 and the whole structure of the advance cybersecurity. In this paper, the key variables are defined. Input and outputs of the proposed model are given in Table 1 and the whole structure of the advance cybersecurity system develops in MATLAB shown in figure

3.2 The Fuzzy Model

Fuzzy logic-based evaluation modelling architecture is given as.

a. Fuzzification: It is the process of generating membership values for a fuzzy variable using membership functions. The first step is to take the crisp inputs (Block Size, Number of Rounds and Key Size) and determine the degree to which the inputs belong to each appropriate fuzzy set. This crisp input is always a numeric value limited to the universe of discourse. Once the crisp inputs are obtained, they are fuzzified against the appropriate linguistic fuzzy sets.
b. Rule evaluation: In this step, the fuzzified inputs are applied to the predecessors of the fuzzy rules.

Since the fuzzy rule has multiple ancestries, a fuzzy operator (AND) is used to obtain a single number that represents the result of the predecessor evaluation. Several rules that created in this evaluation depend on the specification of crypto algorithms, which were derived by mapping three inputs to one output by using a conjunction operator (AND).

c. Aggregation of the rule outputs: The input of the aggregation process is the list of truncated output functions returned by the implication process for each rule. The output of the aggregation process is one fuzzy set for the output variable.

d. Defuzzification: The input for the defuzzification process is a fuzzy set (the aggregate output fuzzy set) and the output is a single number. As much as fuzziness helps the rule evaluation during the intermediate steps, the final desired output for each variable is generally a single number.

3.3 Mamdani Fuzzy Inference System

This system was proposed in 1975 by Ebhasim Mamdani. It was anticipated to control a steam engine and boiler combination by synthesizing a set of fuzzy rules obtained from people working on the system. Steps for Computing the Output Following steps need to be followed to compute the output from this FIS –

Step 1. − Set of fuzzy rules need to be determined in this step.

Step 2. − In this step, by using an input membership function, the input would be made fuzzy.

Step 3. − Now establish the rule strength by combining the fuzzified inputs according to fuzzy rules.

Step 4. − In this step, determine the consequences of rule by combining the rule strength and the output membership function.

Step 5. − Forgetting output distribution combines all the consequents.

Step 6. − finally, a defuzzified output distribution is obtained

The meaning of security risk can be stated as follows. The risk assessment methods have been reported, several searchers. But few kinds of research have challenged the adequacy of this view of risk and emphasized the need to move beyond probability-based perspectives to ones based on uncertainties. Most security risk analysis approaches used in the process industries employ a risk conceptualization similar to that used for safety risk based on representing risk as : Risk = Threat ×vulnerability ×Consequence where, Threat = Probability that an attack occurs, P (A). Vulnerability = Probability that the attack succeeds given that it occurs of conditional probability as P (S | A). Consequence = Expected extent of the impacts given that the attack occurs and succeeds (Q). Quantification of P (A) requires data, knowledge, or modelling of the motivations, intents, characteristics, capabilities, and tactics of adversaries. This poses a considerable challenge and falls largely into the domain of intelligence analysts rather than risk analysts. Quantification of P (S | A) required. Quantification of Q requires capabilities in modelling such phenomena as hazardous material releases, toxic impacts, fires, and explosions. Our main focus is the risk assessment from threat, vulnerability and consequence using the fuzzy logic system. These ideas motivate us to formulate such type model. The flow chart of the proposed model has been depicted in figure 2 the aggregate output fuzzy set and the output is a number. This step was done using the centroid technique because it is the most commonly used method of defuzzification.

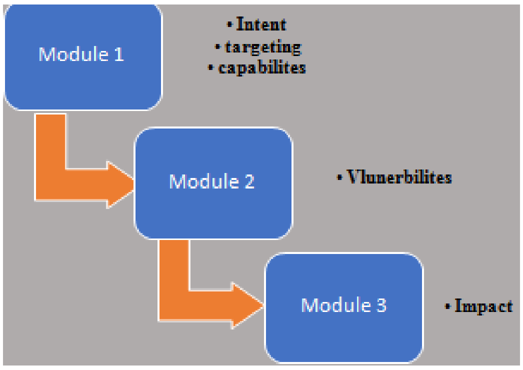


Fig 3: Module of Proposed Algorithm

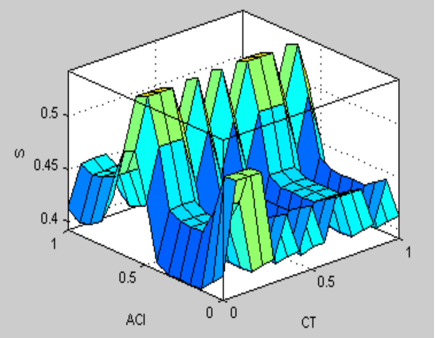


Fig 4: Input variables Cyber Techniques (CT), Aim of Cyber Intruders (ACI) vs. output variable Software (S)

4. SIMULATION AND RESULTS

In this paper, an expert system for cybersecurity based on the 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 83 fuzzy if-then rules were designed for the knowledge base. Input space was divided into multidimensional partitions to formulate the initial rule base. Actions were then assigned to each of the partitions. In advance cybersecurity system fuzzy variables as mentioned, the fuzzy controller also has an advantage of performing according to linguistic rules in the manner of how a human behaves. As shown in Figure 12 cyber techniques (CT) criteria is in the x-axis, advance cyber intruders (ACI) criteria are in the y-axis, and solution criteria software (S) is in the z-axis. It can be seen that cyber techniques (CT) criteria are in the x-axis, advance cyber intruders (ACI) criteria are in the y-axis, and solution criteria user (U) is in the z-axis as shown in Figure

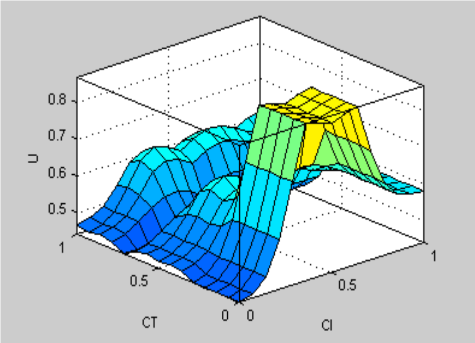
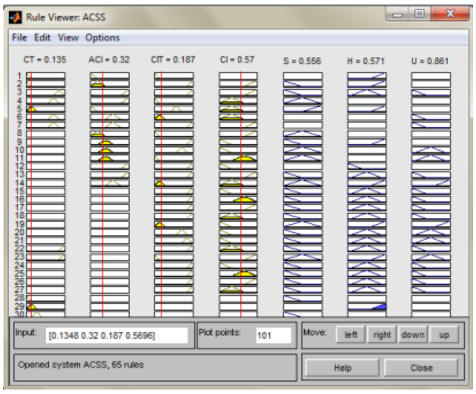


Fig 5: Input Variable, Aim of Cyber intruder Vs Output Variable

e



Input: [0.1348 0.32 0.187 0.5696]

Plot points: 101

Opened system ACSS, 65 rules

Fig6: Fuzzy Rule viewer of Model

5. ACKNOWLEDGMENTS

This research was supported/partially supported by my guide prof. Shital Gupta Assistant Professor SORT (Computer Science Department) Peoples University. We thank my friend from SORT people's university who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. I would also like to show our gratitude to my family sharing their pearls of wisdom with us during this research. Although many errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1]. Martin Botha and Rossouw von Solms" Utilizing fuzzy logic and trend analysis for effective intrusion detection"Elsevier, 2003.

[2]. Shailendra Bajpaia,∗, Anish Sachdevab, J.P. Gupta, "Security risk assessment: Applying the concepts of fuzzy logic", Elsevier,2010

[3]. R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), vol.2, 1, pp. 101-111, 2011.

[4]. R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), vol.2, 1, pp. 101-111, 2011.

[5]. S. M. Bridges, and R. B. Vaughn, "Fuzzy Data Mining And Genetic Algorithms Applied to Intrusion Detection", In Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, 2000, pp.16-19.

[6]. J.T. Yao, S.L. Zhao, and L.V. Saxton, "A Study On Fuzzy Intrusion Detection", In Proceedings of the Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, SPIE, Vol. 5812, Orlando, Florida, USA, 2005, pp. 23-30.

[7]. S. Mukkamala, G. Janoski, A. Sung, "Intrusion detection: support vector machines and neural networks." In: Proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE), St. Louis, MO, 2002, pp. 1702-1707.

[8]. Y. Yu, and H. Hao, "An Ensemble Approach to Intrusion Detection Based on Improved Multi-Objective Genetic Algorithm", Journal of Software, Vol.18, No.6, pp.1369-1378, June 2007.

[9]. J. Cannady, "Artificial Neural Networks for Misuse Detection", in Proceedings of the '98 National Information System Security Conference (NISSC'98), 1998, pp. 443-456.

[10]. W. Lee, S. Stolfo, and K. Mok, "A Data Mining Framework for Building Intrusion Detection Model", In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, 1999, pp. 120-132.

[11]. J. Luo, and S. M. Bridges, "Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection", International Journal of Intelligent Systems, Vol. 15, No. 8, pp. 687-704, 2000.

[12]. C. Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress, Oct. 17, 2003.

[13]. N. Fovino, M. Masera, "A service-oriented approach to the assessment of infrastructure security", in Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, Mar. 19-21, 2007.

[14]. S. M. Furnel and M. J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?" Computers & Security, vol.18, pp.28-34,1999.

[15]. L. Pietre-Cambacedes, T. Kropp, J. Weiss, and R. Pellizzonni, “Cybersecurity standards for the electric power industry-A survival kit,” in CIGRÉ Paris Session, 2008, D2-217.

[16]. R. P. Evans, R. C. Hill, and J. G. Rodriquez, “A Comparison of Cross Sector Cyber Security Standards Idaho National Laboratories”, Idaho National Labs Rep. INL/EXT-05-00656, 2005.

[17]. M. Ferris, "New Email Security Infrastructure", Proceeding of New Security Paradigms Workshop, Aug. 3-5, 1994, pp. 20-27.

[18]. M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, "Distributed network protocol security (DNPSec) security framework", in Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, Arizona, Dec. 5-9, 2005.

[19]. A. Abraham, C. Grosan, C. Martin-Vide, “Evolutionary design of intrusion detection programs.” International Journal of Network Security, vol. 4(3), pp.328-339, 2007.

[20]. W. Chimphlee, A.H. Abdullah, M. N. Sap, S. Srinoy, and S. Chimphlee, "Anomaly-based intrusion detection using fuzzy rough clustering." In Proceedings of the international conference on hybrid information technology (ICHIT'06), 2006, pp. 320-334.

[21]. L. Khan, M. Awad, and B. Thuraisingham. “A new intrusion detection system using support vector machines and hierarchical clustering”, The International Journal on Very Large Data Bases, vol. 16(4), pp.507–521, 2007.

[22]. A.N. Toosi, M. Kahani, “A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Computer Communications, vol.30, pp. 2201-221, 2007.

[23]. A. Tajbakhsh, M. Rahmati, A. Mirzaei, and “Intrusion detection using fuzzy association rules", Applied Soft Computing, Vol: 9, No: 2, pp. 462-469, 2009.

[24]. B. Shanmugam, N. B. Idris, "Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anomaly and Misuse Type of Attacks", in Proceedings of the International Conference of Soft Computing and Pattern Recognition, 2009, pp: 212-217.