Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 15th International Scientific and Practical Conference. Volume II, 259-263

Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection

Krasimir Slavyanov
Department Computer Systems and Technologies
"Vasil Levski" National Military University
Shumen, Bulgaria
k.o.slavyanov@gmail.com

Radostin Dimov
Department Computer Systems and Technologies
"Vasil Levski" National Military University
Shumen, Bulgaria
rsdimov95@gmail.com

Abstract. **This scientific report describes an approach of applying a fuzzy logic decision-making system (Fuzzy Inference System) after detecting a specific cyber incident in a given communication and information infrastructure, supporting the adoption of rapid and adequate measures in the affected systems, both to minimize the consequences for the infrastructure and the functioning of the systems as in general, as well as to support the detailed analysis and prevention of a given cyber incident that has been committed. The cyber security decision-making system was designed in MATLAB's Fuzzy Logic Toolbox, and the input fuzzy variables "Cyber-attack", "Attack Target", "Aim of Attack" were used to select specific action rules. The output fuzzy variables that are designed to produce the result of the operation of the fuzzy rules are: "Hardware actions", "Software actions", "User actions", "Cyber intruder's profile". The purpose of the presented system is to speed up processes after a cyber incident, because delayed and inadequate actions after such an event can lead to an even worse final state of a small or large system, as well as be the cause of great losses for an institution or business. The conducted simulation experiments with different values of the input fuzzy variables prove the approach and the correct decisions that can be made after cyber incidents with different characteristics.**

Keywords: cyber incident, fuzzy inference system, fuzzy logic

I. INTRODUCTION

Artificial Intelligence systems can successfully work in combination with each other [1] and are increasingly used in modern hybrid warfare. In some contemporary studies, the application of interval type-2 fuzzy logic controller for improving risk assessment model of cyber security is proven [2]. The main perspective approaches in assessing risk from intelligent attack are well studied [3]. After the applications of the linguistic variables and the fuzzy logic complex systems for decision processes, the foundation for its application in any human area of activity are open [4], [5]. With the experts' experience and deep study of the logical process of the human decision making the steps for synthesis of the fuzzy logic controller can be determined [6]. Implementation of the fuzzy logic rules with weighted attributes from SIEM database for detection of cyber incidents is successfully proven for special information and communication systems [7] and incident management for technological processes and objects [8]. The multi-criteria decision-making process for cyberattacks can be successfully used with artificial intelligence [9] and the experience about it mentioned before with combination with the contemporary programming languages and experimental environments [10]. The computer network vulnerability estimation [11], cybersecurity recommendations [12] and best practices for any digitalization activities [13] can contribute to cyber experts' decision-making process after common cyber incident detection. If the problems with information security in any communication and information devices are thoroughly investigated and well analysed [14] some new solutions, prevention approaches and standard operational procedures can be invented.

Knowledge of the main cyber-attacks, attack targets, and the aims of attack, in this paper is used for tracing the design process of a fuzzy inference system (FIS) to support rapid and adequate decision-making after a cyber incident such as automating the triggering of standard operating procedures.

II. MATERIALS AND METHODS

The proposed fuzzy inference decision-making system aims to support the overall response of the involved persons such as network administrators and cyber security administrators after the recognition of a given cyber incident in the country's business system. The quick and

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8022

adequate actions indicated by such a system in this direction can reduce the importance of the subjective factor, panic and stress and mark the main mandatory actions to reduce the consequences of the specific cyber incident and direct prevention and preparation in the right direction. The Fuzzy toolbox of MATLAB was used for the working environment of the simulation studies because it offers a sufficiently, reliable, logical, and visual view of the mathematical operations this kind of a study requires (fig.1).

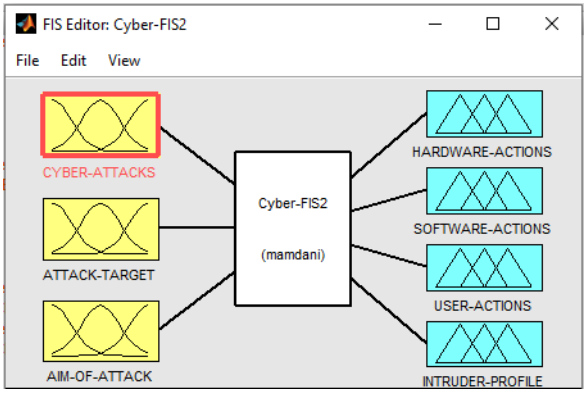

Fig. 1. Fuzzy inference system, designed in MATLAB – Fuzzy Toolbox.

In the selection and summarization of the used input fuzzy variables, the modern state of cyber-attacks, attack targets, aims of attack ware described in Table 1.

For the types of cyberattacks, membership functions are selected, named respectively as commonly accepted concepts in cyber security or their generalizations: "Man in the middle", "DoS, DDoS", "Phishing", "Hack device", "Password", "SQL injection", "Cross-site Scripting", "0 Day", "Malware", "Buffer overflow", "Public Service Exploit". Each of these functions is represented by a Gaussian combination membership function [15] (shown on fig. 2) with a shape corresponding to a smooth increase in the membership value in a separate sector for each of the total 11 and at the same time occupying a large space in the region from 0 to 1 along the vertical to obtain a more categorical result (fig. 3).

As described in Table 1, nine membership functions were designed in a similar way for the varieties of attack targets ("Communication Systems", "Energy /Utilities", "Business", "Healthcare/Medical", "Banking /Financial", "Government", "Military /Police", "Education" and "Transport"), as well as 5 membership functions for the fuzzy variable "Aims of attack" ("Data exfiltration", "Recognition", "Ransom", "System Failure" and "Penetration Test").

TABLE 1 INPUT FUZZY VARIABLES

Input Fuzzy Variables					
Cyber attack		**Attack Target**		**Aim of Attack**	
1	Man in the middle	1	Comm. Systems	1	Data exfiltration
2	DoS,DDoS	2	Energy /Utilities	2	Recognition
3	Phishing	3	Business	3	Ransom
4	Hack device	4	Healthcare /Medical	4	System Failure
5	Password	5	Banking /Financial	5	Penetration Test
6	SQL injection	6	Government		
7	Cross-site Scripting	7	Military /Police		
8	0 Day	8	Education		
9	Malware	9	Transport		
10	Buffer overflow				
11	Public Service				

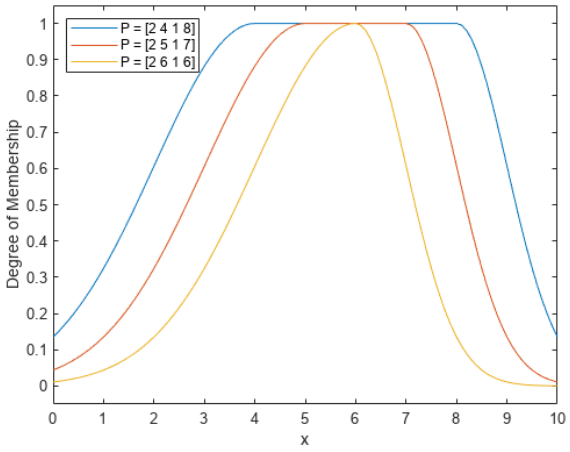

Fig. 2. Gaussian combination membership function [15]

The initial fuzzy variables described in Table 2, may contain several analytical data that can be obtained if the input fuzzy variables discussed are properly analysed. These variables summarize the essential and expertly required actions after the recognition and identification of a cyber incident. The areas of action by the responsible personnel or specialized software are summarized in 3 areas – hardware actions, software actions and user actions.

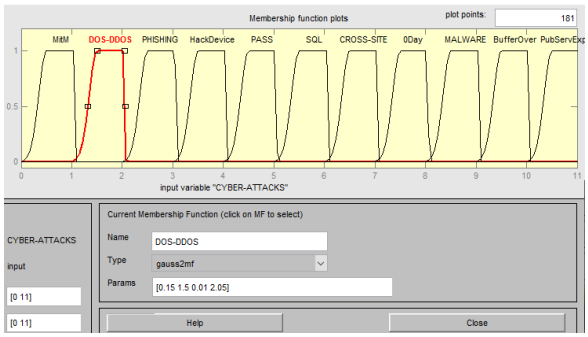

Fig. 3. Membership functions of the fuzzy variable "Cyber attacks".

TABLE 2 OUTPUT FUZZY VARIABLES

Output fuzzy variables							
Hardware actions		**Software actions**		**User actions**		**Cyber intruder's profile**	
1	Physical control	1	Special Software	1	End-User Training	1	Insider
2	Dedicated Systems / DMZ	2	WAF / Network Firewall – reconfiguration	2	Situation Awareness	2	Black hat Hacker
3	Special Technical support	3	SIEM reconfiguration	3	User control update	3	Purple Hat Hacker
4	System Isolation	4	System Update			4	Ethical Hacker
		5	SOP for the attack			5	Cyber Activist
		6	Backup /Restore				

While the first 2 refer to the technical systems, the actions with the users require assistance from the HR structure or the ERP system. In detail, the description of the specific actions is as follows:

A. Hardware actions:

- Physical control – restoration and improvement of physical access control systems to communication and information resources, as well as to specialized equipment.
- Dedicated Systems / DMZ – Designation of Dedicated computer Systems for the specific affected critical systems or construction of a demilitarized zone to restrict access and control.
- Special Technical support – when the intervention of a higher-level specialist is required for the specific system.
- System Isolation – isolation of the affected element from the entire system, if possible, for subsequent thorough analysis of the attack and the affected resources.

B. Software Actions:

- Using specialized software or improving it for its specific activity from the point of view of cyber security.
- WAF / Network Firewall – reconfiguration.
- SIEM reconfiguration.
- System Update - to install the latest security packages.
- SOP for the attack – creation of standard operating procedures (or a software program) to determine the mandatory steps of work in case of repeating an incident of the same type.
- Backup/Restore – Building a reliable system for Backup/Restore, for fast recovery and minimal loss of operational data.

C. Actions with affected user personnel:

- Organization of specialized cyber security training for end users.
- Situation Awareness – correct understanding of the situation and orientation in the new environment.
- User control update – improvement of the employee behaviour control system.

One of the important things that can also be analysed based on the input fuzzy variables described before is the intruder profile - as an output variable of the FIS, which, with certain generalizations can take the following values, designed as membership functions:

- Insider – a person with access to the corporate network and resources and sufficient skills.
- Black hat Hacker – the real criminal.
- Purple hat hacker – people who are only testing and improving their hacking skills.
- Ethical hacker – expert in cybersecurity and cyber defence.
- Cyber activist – someone who uses their skills to hack various systems to practice any type of activism.

For tighter coverage, a membership function of type gbellmf is chosen for all the set possible output values. This function computes fuzzy membership values using a generalized bell-shaped membership function as is shown on fig 4 [16].

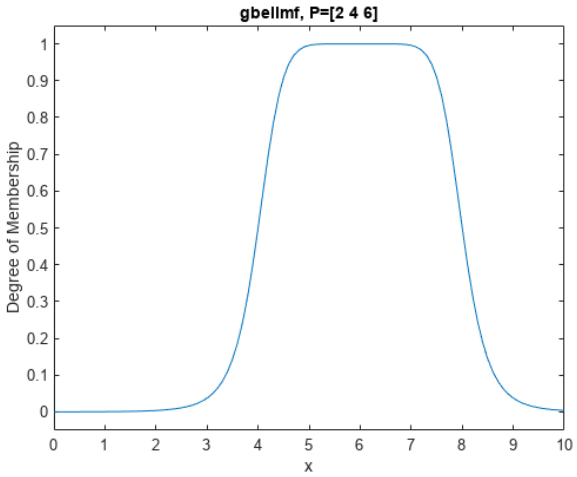

Fig. 4. Gaussian combination membership function [16]

The Membership function of the output fuzzy variable "Hardware actions" is depicted on fig.5.

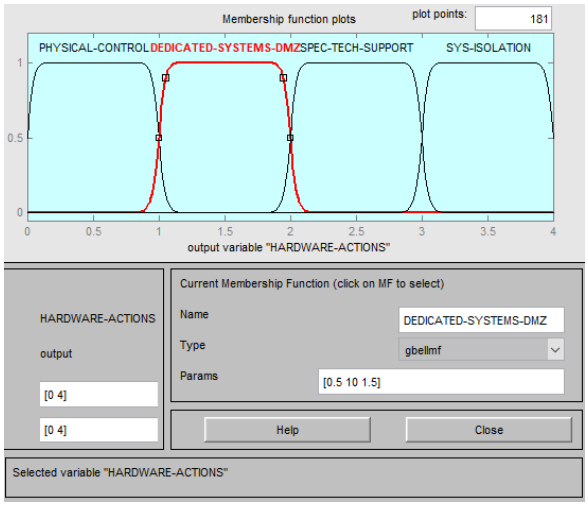

Fig. 5. Membership function of the output fuzzy variable “Hardware actions”.

For this project, the input and output fuzzy variables, a system of 184 example fuzzy rules is created, combining all variables to obtain results for the three categories of FIS output (fig.6 and fig.7). More rules created can lead to computer system limitations being reached.

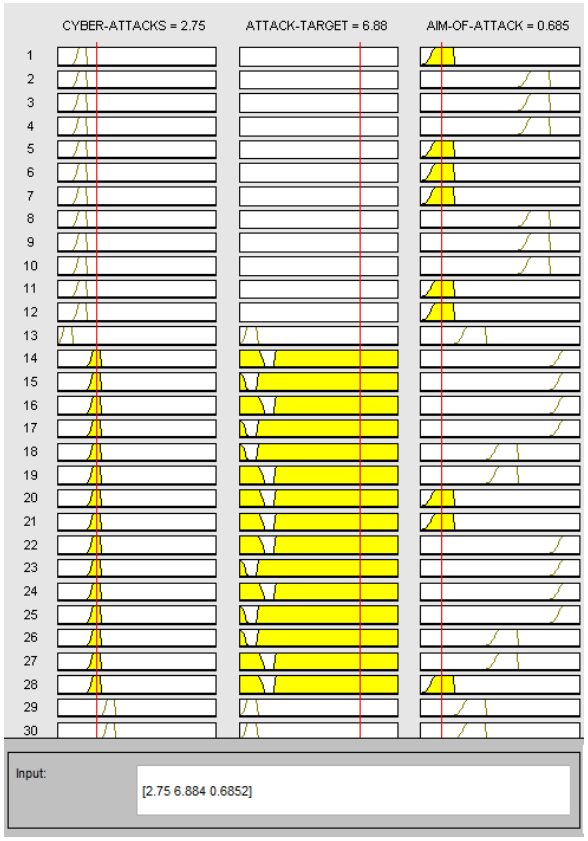

Fig. 6. Input variable values fallen in the 184 rules (first 30 are depicted).

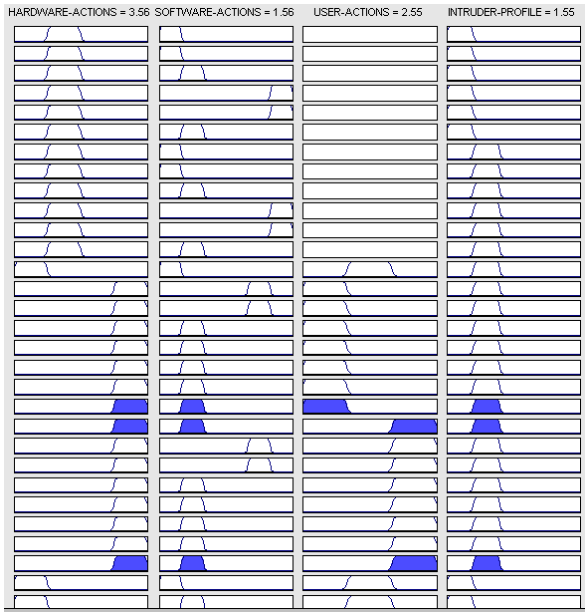

Fig. 7. Output values of variables after running 184 rules (the results of the first 184 rules are shown).

III. Results and Discussion

The more and more precise fuzzy rules are created, the more precise and definite the results will become. With set implication method = min, aggregation = max type of defuzzification - last of maxima, the obtained results, visible from the surface (Fig. 8), are clearly defined.

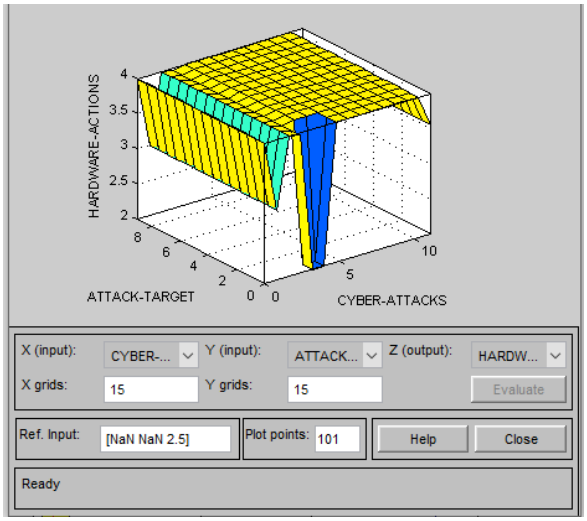

Fig. 8. Output fuzzy variable "Hardware actions".

For the specific example with input fuzzy variables "Cyber-attacks" = 2.75 (Phishing), "Attack targets" = 6.884 (Military Police) and "Aims of attack" = 0.6852 (Data Exfiltration), fuzzy rules form output values of the variables as follows: "Hardware actions" = 3.56 (System isolation), "Software actions" = 1.56 (WAF/Network Firewall – reconfiguration), "User actions" = 2.55 (User control update) and "Cyber intruder's profile" = 1.55 (Black hat Hacker).

IV. Conclusions

The application of the Fuzzy inference system of the Mamdani type, for the needs of post cyber incident action can be particularly applicable, given the different nature of

the input linguistic variables and the special place that is assigned to systems of this type, namely in solving security crises, as the values of the input variables for a FIS could be fed as outputs from a deep learning system. The structure of a practical approach for a system of standard operating procedures after a cyber incident based on the proposals in this document should be continuously adapted and changed to achieve the set and objectives, given the rapidly changing cyber threats.

ACKNOWLEDGMENTS

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

[1] K. Slavyanov, C. Minchev, „An Algorithm of Fuzzy Inference System for ISAR Image Classification“, Environment. Technology. Resources, Rezekne, Latvia, Proceedings of the 11th International Scientific and Practical Conference., 2017, Volume II, pp 154-158, https://doi.org/10.17770/etr2017vol2.2599

[2] D. K. Jana and R. Ghosh, "Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security" , Journal of Information Security and Applications, 2018, 40, pp. 173–182. https://doi.org/10.1016/j.jisa.2018.04.002

[3] S. D. Guikema and T. Aven, "Assessing risk from intelligent attacks: A perspective on approaches", Reliability Engineering & System SafetyVolume 95, Issue 5, May 2010, pp. 478-483, https://doi.org/10.1016/j.ress.2009.12.001

[4] L.A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning—I", Information Sciences 8, 1975, pp. 199-249.

[5] L.A. Zadeh, "Outline of a new approach to the analysis of complex systems and decision processes", IEEE Transactions on Systems, Man, and Cybernetics, Vol. 3, No. 1, Jan. 1973, pp. 28-44.

[6] E.H. Mamdani, S. Assilian, An experiment in linguistic synthesis with a fuzzy logic controller, International Journal of Man-Machine Studies, Vol. 7, No. 1, 1975, pp. 1-13. https://doi.org/10.1016/S0020-7373(75)80002-2

[7] I. Subach and I. Parashchuk, “Methodology of formation of fuzzy associative rules with weighted attributes from SIEM database for detection of cyber incidents in special information and communication systems”, Chapter in book: Advances in Automation II, March 2021, https://doi.org/10.20535/2411-1031.2023.11.1.283575

[8] I. Subach and I. Parashchuk, “A Fuzzy Model of the Security Event and Incident Management for Technological Processes and Objects”, book: Advances in Automation II, March 2021, pp 550–559, https://doi.org/10.1007/978-3-030-71119-1_54

[9] A. Bouramdane, Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process, September 2023, Journal of Cybersecurity and Privacy 3(4), https://doi.org/10.3390/jcp3040031

[10] A. Borisova, “Contemporary languages for programming artifical intelligence”, International Scientific Conference "Defense Technologies" 2019, pp. 512-517, ISSN 2815-4282, https://www.aadcf.nvu.bg/scientific_events/dtf2019/AngelaRBorisova.pdf [Accessed Jan 10, 2024]

[11] L. Nikolov, "Wireless Network Vulnerabilities Estimation", International Scientific Journal "Security and Future", Vol. 2 (2018), Issue 2, pp. 80-82, https://stumejournals.com/journals/confsec/2018/2/80.full.pdf [Accessed Jan 18, 2024]

[12] M. Nedelchev and D. Slavov, “Cybersecurity recommendations and best practices for digital education”, Scientific research and education in the air force, 2023, pp. 47-52, https://doi.org/10.19062/2247-3173.2023.24.6

[13] Y. Dechev, “Research on the impact of online learning on individual learning styles”, Mathematics and informatics, April 2023, Volume 66, issue 2, pp 155-169. https://doi.org/10.53656/math2023-2-5-res

[14] V. Stoyanova, “Problems with information security on mobile devices”, International Scientific Journal "Industry 4.0", WEB ISSN 2534-997X; print ISSN 2534-8582, Year IV, Issue 4, 2019, pp. 200-202, https://stumejournals.com/journals/i4/2019/4/200

[15] Mathworks support documentation, Fuzzy Toolbox, gauss2mf https://www.mathworks.com/help/fuzzy/gauss2mf.html [Accessed Jan 18, 2024]

[16] Mathworks support documentation, Fuzzy Toolbox, gbellmf, https://www.mathworks.com/help/fuzzy/gbellmf.html [Accessed Jan 18, 2024]