ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse145942020.pdf
https://doi.org/10.30534/ijatcse/2020/145942020

The Production Model of Fuzzy Neural Network in Information Security Systems

Zyryanov S. I.[1], Berezhnov V. P.[2], Perepelkina Yu. V.[3], Shevtsov A. I.[4], Shevchenko K. K.[5], Kozlov V. V.[6]
[1]Department of Higher mathematics and natural science, synergy University, Moscow, Russia
[2]Department of Higher mathematics and natural science, synergy University, Moscow, Russia
[3]Department of Higher mathematics and natural science, synergy University, Moscow, Russia
[4]Department of Higher mathematics and natural science, synergy University, Moscow, Russia
[5]Department of Higher mathematics and natural science, synergy University, Moscow, Russia
[6]Department of Higher mathematics and natural science, synergy University, Moscow, Russia

ABSTRACT

In this article, a model for evaluating the level of information security based on a fuzzy neural production network is proposed. The methodology of qualitative assessment of the level of information security in the system is based on the results of measurements and expert assessments, which may be unclear and insufficiently expressed in order to be described by mathematical dependencies. The functional status of such systems can be described using fuzzy rule constructs. Fuzzy production networks are identical in their structure to multilayered neural networks, and this property was applied by the authors to construct a neural network model for evaluating the level of information security. The concept of technological security profiles is introduced as a set of security States that correspond to the identified technical channels of information leakage at a certain time. It is proposed to rank these channels by importance before processing in the neuro marketing system.

The results obtained allow us to formulate directions for further research on the development of new effective information protection systems using intelligent technologies.

Key words : information security, fuzzy production models, neuron, neuronal network, technological portrait of security, technical channel of information leakage.

1. INTRODUCTION

A set of security States that correspond to the technical channels of information leakage detected on the OID at a certain time can be represented as dynamic systems. These States are called events and are represented as technological portraits of the protected environment [1-4]. This term, which covers the corresponding concepts of a physical, informational and secure nature, refers to the occupation of a dynamic distributed network of a certain technological state or configuration of States [5]. The evolutionary changes that take place between stages are not taken into account and it is assumed that the dynamics of the system develops discretely, from event to event. Such a system is discrete-mode [5].

The environment for a neural network system (NMS) to assess the level of information security can be represented as a set of discrete-mode systems with associated discrete technological States of security [6-9].

Getting the necessary number of instrumental measurements and special studies for each of the technical channels of information leakage received on the OID, neo needs to develop such a procedure for processing measurements, which allows you to automatically receive information about the technological state of security of each of the channels according to the approved threat model [10].

2. MATERIALS AND METHODS

The results of instrumental measurements and special ossiers for each of the technical channels of information leakage are perceived by the sensor matrix in the form of a set of observations [11-13]:

X =(X X1, 2,..., Xi,..., Xm), and = 1,2,...,n.

In a separate sensor channel, a reduction of the sample space X occurs, y resulting in a sequence of discrete variables Uk, k = 0,1,..., n-1, which take the values Z1, Z2,..., Zr.

It is necessary to synthesize the structure of a neuropod-like classifier that implements the crucial function $\gamma(U)$ on the reduced sample space U [6].

The sequence of discrete variables Ur, k = 0,1,..., n-1, which take the value z, a = 1,2,..., r, can be approximated by vectors Ξ, f(0)μ and Ξ,

F (k)μ.

The structure of the simplest neural network-like security assessment system is a set of M+1 ensembles of first-layer neural networks . The ensemble consists of n-neurons, whose excitation level is defined as n [14]

Yμ(k)=∑Ξa(k)Fa(k)μ a=1 ,

where Ξ, f(0)μ and Ξ, f (k)μ. - vectors that can be used to approximate a sequence of discrete variables Ur, k = 0,1,..., n-1, takes the values za, a = 1,2,...,r [5].

Each neuron carries out encoding process, which is determined by the so-called method of labeled lines, wherein the particular value the process provided in accordance specific (labeled) line Z1,Z2,...,Z,a,...,Zk , and hence the specified value of the process parameter corresponds to one maximum excited synaptics the connection a (k) =1 [15].

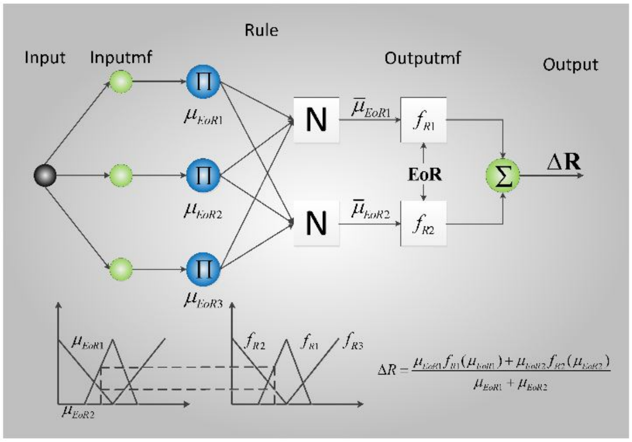

Figure 1: Fuzzy logic neural network-based in information security system

Figure 1 shows us fuzzy logic neural network.In contrast to a typical neuron, whose synaptic connections are equivalent, a neuron that encodes by the method of labeled lines has priority synaptic connections. A synaptic input with a larger number corresponds to a larger value of the process parameter. Another difference is that k only one synaptic link is triggered at the k-th instant of time, and thus the task of entering and controlling the threshold Θ, using the weight function w , is greatly simplified w [16-18].

For each technical channel in the set {ml}TKVI it is necessary to determine its importance [8].

Despite the difference in the number of threats in accordance with [5], which define each possible technical channel, this number does not determine the degree of danger of the technical channel itself. Therefore, to determine the importance coefficients, it is rational to use the ratio between the total number of threats of a particular channel and the number of threats that took the value " 1 " according to the results of an expert survey [19].

Then the formula for determining the importance coefficients of each technical channel in the list looks like this:

M1 ll = Mll , l =1..L

where Ml1 - the number of threats of the l–th technical channel, which took the value “1” according to the results of an expert survey; Ml-the total number of threats that characterize the l-th technical channel [20].

Thus, a set of values for the importance of each possible technical channel is formed information leaks - {λl}TKVI, l =1,L . The synaptic input with a high number corresponds to the value of the parameter of the technical channel with a high rating.

It is necessary to conduct an inventory of technical channels of importance and form a final list of possible technical channels for information leakage to the OID [21-24]:

{ml}TKVI, l =1, ,L where L ≤ 8.

The proposed approaches allow us to formalize, for example, the results of further research on the development of new effective information security systems using intelligent technologies.

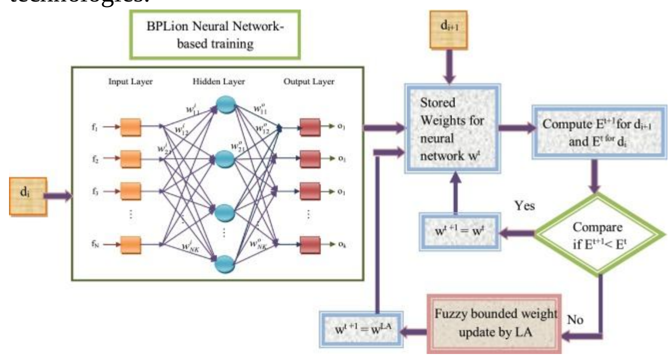

Figure 2: Training of neural network for security dimension

Figure 2 shows us training of neural network and algorithms. The difference between it and existing systems for assessing the level of security that the neural network structure is focused on solving a specific task – creating and certifying an object of information activity or creating a comprehensive information security system in its. The requirement of problem orientation of the neural network (NM) leads to the implementation of the principle of adequacy of its structure and external environment, i.e. the possibility of flexible structural and functional adjustment [25]. This determines the most important property of NM-adaptability to changes in the environment of its functioning, which is very relevant for the complexityof the structure of modern its. The initial structuring of the neural network should be carried out by formal synthesis methods, which determine the optimal structure, including the number of neural layers and neural ensembles, the number of neural-like elements in each layer, and the presence of deterministic elements links between them and the initial weight coefficients [22].

3. CONCLUSION

The current novelty of the work is to expand the understanding of cloud computing, review the requirements for both methods and forms of organizing scientific research, preserving scientific information and sharing it, and in the role of a scientist and his professional ICT competencein organizing scientific work.

REFERENCES

1. Ahmed M, Litchfield AT (2018) **Taxonomy for identification of security issues in cloud computing environments**. J Comput Inf Syst 58(1):79–88
2. Anisetti M, Ardagna C, Damiani E, Gaudenzi F (2017) **A semi-automatic and trustworthy scheme for**

continuous cloud service certification. IEEE Trans Serv Comput 10(1):1–14

3. Annette JR, Banu WA, Chandran PS (2015) **Rendering-as-a-service: taxonomy and comparison**. Procedia Comput Sci 50:276–281 https://doi.org/10.1016/j.procs.2015.04.048
4. Apps Run The World (2017) **Cloud applications revenue from leading vendors worldwide in 2015 and 2016 (in million U.S. dollars)**. https://www.statista.com/statistics/475844/cloud-applications-revenues-worldwide-by-vendor/.
5. Cloudscene (2018) **Top ten data center operators in North America**, EMEA, Oceania and Asia for the January to March 2018 period. https://cloudscene.com/top10
6. Dašić P, Dašić J, Crvenković B (2016) **Service models for cloud computing: search as a service (SaaS).** Int J Eng Technol (IJET) 8(5):2366–2373
7. Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM (2014) **Security issues in cloud environments: a survey**. Int J Inf Secur 13(2):113–170
8. Gao F, Thiebes S, Sunyaev A (2018) **Rethinking the meaning of cloud computing for health care: a taxonomic perspective and future research directions.** J Med Internet Res 20(7):e10041
9. Grozev N, Buyya R (2014) **Inter-cloud architectures and application brokering: taxonomy and survey**. Softw Pract Exp 44(3):369–390 https://doi.org/10.1002/spe.2168
10. ITCandor (2018) **Distribution of cloud platform as a service (PaaS) market revenues worldwide from 2015 to June 2018, by vendor**. https://www.statista.com/statistics/540521/worldwide-cloud-platform-revenue-share-by-vendor/
11. Khan N, Al-Yasiri A (2016) **Identifying cloud security threats to strengthen cloud computing adoption framework**. Procedia Comput Sci 94:485–490
12. Lins S, Schneider S, Sunyaev A (2018) **Trust is good, control is better: creating secure clouds by continuous auditing.** IEEE Trans Cloud Comput 6(3):890–903
13. Lins S, Schneider S, Szefer J, Ibraheem S, Sunyaev A (2019) **Designing monitoring systems for continuous certification of cloud services**: deriving meta-requirements and design guidelines. Commun Assoc Inf Syst 44:460–510
14. Schneider S, Sunyaev A (2016) **Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing**. J Inf Technol 31(1):1–31
15. Singh A, Chatterjee K (2017) **Cloud security issues and challenges: a survey**. J Netw Comput Appl 79(C):88–115
16. Stephanow P, Banse C (2017) **Evaluating the performance of continuous test-based cloud service certification**. Paper presented at the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, Madrid, 14–17 May 2017 https://doi.org/10.1109/CCGRID.2017.134
17. Stephanow P, Khajehmoogahi K (2017) **Towards continuous security certification of software-as-a-service applications using web application testing techniques**. Paper presented at the 31st IEEE international conference on advanced information networking and applications, Taipei, 27–29 Mar 2017
18. Glebova, I. S., Kotenkova, S. N., & Abramov, R. A. (2016). **The analyses of socio-economic development tendencies of the capital cities in the modern Russia**. In Social Sciences and Interdisciplinary Behavior - Proceedings of the 4th International Congress on Interdisciplinary Behavior and Social Science, ICIBSOS 2015 (pp. 189–194).
19. Ivanovich, G. V, Aharonovich, A. R., & Sergeevich, S. M. (2019). **Implementation of international experience in support of youth innovative entrepreneurship in the Union state**. Academy of Entrepreneurship Journal, 25(Special Issue 1).
20. Klyuev S.V., Bratanovskiy S.N., Trukhanov S.V., Manukyan H.A. **Strengthening of concrete structures with composite based on carbon fiber** // Journal of Computational and Theoretical Nanoscience. 2019. V.16. №7. P. 2810 – 2814.
21. Shashkova, A., Verlaine, M., & Kudryashova, E. (2020). **On modifications to the constitution of the russian federation in 2020**. Russian Law Journal, 8(1), 60–83. https://doi.org/10.17589/2309-8678-2020-8-1-60-83
22. Shashkova, A. (2019). **Regulating principles of disclosure of information to shareholders under G20** / OECD principles. In Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020 (pp. 1931–1936).
23. Gennadievich, B. A. (2020). **Machine learning and data mining activity results when using projectiles in different sports**. International Journal of Advanced Trends in Computer Science and Engineering, 9(3), 3157–3160. https://doi.org/10.30534/ijatcse/2020/103932020
24. Uzougbo, I., Onwuegbuzie, Razak, S. A., Isnin, I. F., & Latiff, N. A. A. (2019). **Routing protocol for low-power and lossy network performance comparison for objective functions.** International Journal of Advanced Trends in Computer Science and Engineering, 8(1.6 S1), 109–115. https://doi.org/10.30534/ijatcse/2019/1781.62019
25. Vaghashiya, R., Thakore, R., Patel, C., & Doshi, N. (2019). **IoT – principles and paradigms**. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.6 Special Issue), 153–158. https://doi.org/10.30534/ijatcse/2019/2481.62019