Analysis of Cloud Biomedical Healthcare Systems Security Based on Matrix Rewriting SRNs With Fuzzy Parameters

Victor Moraru[1], Alexei Sclifos[1], Simion Cuzmin[1], Emilian Guțuleac[1]
[1]Technical University of Moldova, Bd. Ștefan cel Mare, 168, MD-2004, Chișinău, R. Moldova, victor.moraru@calc.utm.md, ORCID: 0000-0002-5454-8341, 0000-0003-4531-7944, 0009-0006-4698-0341, 0000-0001-6839-514X, https://utm.md

Keywords: — cloud biomedical healthcare systems security, fuzzy numbers, moving target defense, performability modeling, rewriting rules, stochastic Petri nets

Abstract. Cloud-based Biomedical and Healthcare Systems (CBHS) play an important role in providing access to services for solving widespread problems related to biomedical complications [1]. The sensitive nature of data in CBHS presents considerable challenges regarding its security and privacy, at the same time, CBHS are more susceptible to cyber-attacks compared to conventional computer systems. One of the key functions of the CHBS is the centralized data processing using cloud computing technologies. The aims of this article are the modelling and analyzing of the defense process against cyber-attacks in CBHS.

To address this issue, recently are proposed an emerging proactive defense approach, the Moving Target Defense (MTD) techniques, that aims to thwart attacks by dynamically changing the attack surface and disrupts the attacker's exploration phase [3], leading to complexity and unpredictability, thus confusing attackers by creating asymmetric uncertainties in favor of the defenders, thus reducing the probability of the success of an attack. However, migration services from one cloud Virtual Machines (VMs) to another in the CBHS takes a finite time that delays the service execution and leads to the degradation of its performances. So, we need to evaluate and analyze the impact of using an MTD technique for CBHS defense under uncertainty. We used as mathematical formalism the Stochastic Reward Nets (SRNs) [4], a variant of stochastic Petri nets, because it is conceptually easy to understand

due to its graphical nature and it is well supported by the theory, as well by a large number of existing software tools.

Nevertheless, in this type of models, the fuzzy epistemic uncertainties of the attacker's behavior are not taken into account. So, it is necessary to enhance the SRN in order to fully represent more compactly and flexibly the models that describe complex processes of CBHS and also to evaluate the impact of MTD migration policies in terms of performability.

In this paper we propose the Matrix Rewriting SRNs (MRSRN) with Fuzzy parameters (FMRSRN) for properly uncertainty performability modeling and analysis of CBHS that are enhanced with time-based MTD techniques. One of the key advantages of utilizing FMRSRN for CBHS modeling is that these models have a compact structure, making them flexible for reconfiguration and modification of quantitative parameters during runtime.

The implementation of the suggested FMRSRN method is illustrated through a performability modeling and numerical case study analysis of a specific CBHS.

References

[1] B. Guo, N. S. Ahmad Shukor, I. S. Ishak, "Enhancing healthcare services through cloud service: a systematic review", *International Journal of Electrical and Computer Engineering*, Vol. 14, No. 1, pp. 1135–1146, 2024.

[2] M. Aijaz, M. Nazir, M. N. Mohammad, "Threat Modeling and Assessment Methods in the Healthcare-IT System: A Critical Review and Systematic Evaluation", *SN Computer Science* 4:714, pp.1–21, 2023.

[3] J. Zheng, A. S. Namin, "A survey on the moving target defense strategies: An architectural perspective", *Journal of Computer Science and Technology*, 34(1), pp. 207–233, 2019.

[4] J. Muppala, G. Ciardo, and K. S. Trivedi, "Stochastic reward nets for reliability prediction", *Commun. Reliab. Maintainab. Serv.*, vol. 1(2), pp. 9–20, 1994.