*Journal of Engineering Science* *Vol. XXXII, no. 3 (2025), pp. 64 - 74*
*Fascicle* *Electronics and Computer Science* *ISSN 2587-3474*
*Topic* *Biomedical Engineering* *eISSN 2587-3482*

**https://doi.org/10.52326/jes.utm.2025.32(3).06**
**UDC 004.056.5:004.7:614.2:519.8**

# ANALYSIS OF CLOUD BIOMEDICAL HEALTHCARE SYSTEMS SECURITY BASED ON MATRIX REWRITING SRNS WITH FUZZY PARAMETERS

Victor Moraru *, ORCID: 0000-0002-5454-8341,
Alexei Sclifos, ORCID: 0000-0003-4531-7944,
Simion Cuzmin, ORCID: 0009-0006-4698-0341,
Emilian Guțuleac, ORCID: 0000-0001-6839-514X

*Technical University of Moldova, 168, Ștefan cel Mare Blvd., Chisinau, Republic of Moldova*
* Corresponding author: Victor Moraru, *victor.moraru@calc.utm.md*

Received: 07. 12. 2025
Accepted: 08. 14. 2025

**Abstract.** This paper presents an analytical uncertainty performability, (especially the security) analysis of Cloud Biomedical Healthcare Systems (CBHS) Security based on Matrix Rewriting Stochastic Reward Nets with Fuzzy parameters (FMRSRN), that allows the compact modeling and evaluation of the impact in which is used a proactive defense time-based Moving Target Defense (MTD) technique. A numerical case study for performability modeling and analysis of a particular CBHS is given to show the effectiveness of proposed method.

**Keywords:** *cloud biomedical healthcare systems security; fuzzy numbers; moving target defense; performability modeling; rewriting rules; stochastic Petri nets.*

**Rezumat.** Această lucrare prezintă o analiză a performabilității (în special a securității) in condiții de incertitudine a securității sistemelor biomedicale de sănătate implementate în cloud (CBHS) bazată pe rețele stocastice cu recompensă cu parametri fuzzy (FMRSRN), care permite modelarea compactă și evaluarea impactului utilizării unei tehnici de apărare proactivă bazate pe deplasarea in timp a țintelor mobile (MTD). Este prezentat un studiu de caz numeric pentru modelarea și analiza performabilității unui sistem CBHS pentru a demonstra eficacitatea metodei propuse.

**Cuvinte cheie**: *securitatea sistemelor biomedicale de sănătate în cloud; numere fuzzy; apărare prin ținte mobile; modelare a performanței; reguli de rescriere; rețele Petri stocastice.*

## 1. Introduction

Cloud-based Biomedical and Healthcare Systems (CBHS) are essential for delivering services that address common challenges associated with biomedical issues [1,2]. At the same time, these services facilitate the sharing and use of biomedical and healthcare resources, improve their efficiency and quality, reduce costs, improve people's health and access to biomedical data. However, the sensitive nature of biomedical healthcare data poses significant challenges to its security and privacy in the CBHS [3-5]. Thus, in addition to the

many advantages of CBHS for our health, they are more vulnerable to cyber-attacks than traditional computer systems.

To tackle this challenge, a new proactive defense strategy known as Moving Target Defense (MTD) has recently been introduced. MTD works by continuously altering the attack surface, thereby interrupting the attacker's reconnaissance efforts [6,7]. This approach increases system complexity and unpredictability, generating asymmetric uncertainty that benefits the defenders and decreases the likelihood of a successful attack. However, transferring CBHS services between cloud Virtual Machines (VMs) requires a finite amount of time, which can delay service execution and negatively impact overall performance.

Performability is the emerged metric to evaluate the ability of a system to function when its system's performances degrade regarding how well it executes its specified functionalities under normal and abnormal conditions in the presence of system failures, vulnerabilities and security threats and intruders' attacks [8]. In this article, we will often use the term performability as synonym of the security term, one of the well-known performability metrics.

In this context, there is a need to evaluate and analyze the impact of using an MTD technique for CBHS defense on the specified performability metrics under uncertainty. Thus, the CBHS behavior modeling and performability evaluation must be proven by adopting and using some mathematical formalisms. Amongst such formalisms, the Stochastic Reward Nets (SRNs) [9], a variant of stochastic Petri nets, are widely used because they are conceptually easy to understand, graphical in nature and well supported by a large body of theory as well as a large software tool base.

Most of the existing research based on SRN models, focuses only on the evaluation of MTD techniques impact on the system security, but not on investigating the effects considering the potential performance degradation due to the MTD launched in computing systems [6,7]. However, these types of models do not consider the fuzzy epistemic uncertainties related to attacker behavior. Additionally, Stochastic Reward Nets (SRNs) can be challenging to apply in real-world scenarios because the graphical representation of real systems tends to grow rapidly in size. Therefore, it is essential to improve SRNs to enable a more compact and flexible representation of complex CBHS processes, while also allowing for the evaluation of MTD migration policies in terms of system performability.

In this paper, we introduce Matrix Rewriting SRNs (MRSRN) with Fuzzy parameters (FMRSRN) as a suitable approach for modeling and analyzing the uncertainty and performability of CBHS enhanced with time-based MTD techniques. One of the key advantages of using FMRSRN for CBHS modeling is its highly compact and adaptable structure, which allows for easy reconfiguration and dynamic adjustment of quantitative parameters during runtime.

The application of the proposed FRSRN approach is exemplified by performability modeling and numerical case study analysis of a particular CBHS.

## 2. Matrix rewriting SRN with fuzzy parameters

### *A. Epistemic Uncertainty **and Fuzzy Numbers***

In a complex real system, the accurate evaluation of performability metrics is difficult due to several sources of uncertainties: aleatory that refers to probabilistic variations in a random events, epistemic that comes from lack of knowledge, e.g. inadequate and/or incomplete understanding of the processes, technical restraints, ambiguous information,

imprecise values of input parameters, etc. Therefore, the uncertainty modeling of CBHS behavior can be treated more realistically through FRSRNs that the transition firing rates can be considered as fuzzy numbers. Next, with the goal to facilitate the exposition of the proposed approach, we present some basic elements of fuzzy sets and fuzzy numbers (FN) [10,11] for defining FMRSRN.

A fuzzy subset $\widetilde{A}$ of the real numbers set $IR$ is defined by its membership function $\mu_{\widetilde{A}} : IR \to [0,1]$ which assigns a real number $\mu_{\widetilde{A}}$ in the interval $[0,1]$ to $\forall \widetilde{x}$, where the value of $\mu_{\widetilde{A}}$ at $x$ shows the grade of membership function of $x$ in $\widetilde{A}$.

The triangular fuzzy numbers (TFN) are often used in real applications. A TFN is described as $\widetilde{a} = (a, \delta, \beta)$ where $a$ is the *center*, $\delta$ is the *left width*, and $\beta$ is the *right width*. For arbitrary fuzzy number $\widetilde{a} = (a, \delta, \beta)$, the membership function is equal:

$$\mu_{\widetilde{a}}(x) = \begin{cases} 1-(a-x)/\delta, & a-\delta \le x \le a, \\ 1-(x-a)/\beta, & a \le x \le a+\beta, \\ 0, & otherwise. \end{cases}$$

However, a parametric $\alpha - cut$ fuzzy number $\widetilde{a} = [a^{-}(\alpha), a^{+}(\alpha)]$ can be represented as: $a^{-}(\alpha) = a - (1-\alpha)\delta$ and $a^{+}(\alpha) = a + (1-\alpha)\beta$.

### *B.* ***Basic Concepts and Elements of FMRSRN***

We assume that readers already have a foundational understanding of the core principles and behavioral rules of SRNs. A thorough theoretical discussion and practical application of this subject fall beyond the scope of this paper. For more in-depth information on SRNs, readers are encouraged to consult reference [9]. In this subsection, we offer a concise overview of the FMRSRN.

Let $IN_{+}$ (resp. $IR^{+}$) is a pair of *natural* (resp. positive *real*) numbers.

The definition of an FMRSRN is derived according to [12,13] and inherits most of the Rewriting SRN and MRSRN characteristics. Thus, the FMRSRN, denoted $\Gamma FR$, is defined as a 14-*tuple* system such that $\Gamma FR = < P, T, R, A_{rcs}, \Pr i, G^{E}, G^{R}, Kp, \widetilde{\Lambda}, \widetilde{\omega}, \widetilde{\rho}, M_0, Lib_R, Lib_{At} >$, where: $P$ (resp. $T$) is a finite set of *places* (resp. *transitions*); $R$ is a finite set of *rewriting rules* about the *run-time structural change* (*reconfiguration*) of $\Gamma FR$ net. Let $E = T \cup R$ be a finite set of events, $T \cap R = \varnothing$, $P \cap E = \varnothing$. The set $E$ is partitioned into $E = E_0 \cup E_\tau$, $E_0 \cap E_\tau = \varnothing$ so that: $E_0$ is a set of immediate events and $E_\tau$ is a set of timed events; $A_{rcs}$ = < *Pre*, *Post*, *Inh, Test* > is a set of *forward*, *backward, inhibition* and *test* (*promoter*) arc functions with respective weight cardinalities; *Pri* is the dynamic priority function for the *firing* of each *enabled* event. By default, $\Pr i(E_0) > \Pr i(E_\tau)$; $G^{E} : E \times IN_{+}^{|P|} \to \{True,\ False\}$ (resp. $G^{R} : R \times IN_{+}^{|P|} \to$ {*True*, *False*}) is the set of *guard function* associated with all event $e \in E$ (resp. *rewriting rule* $r \in R$); $K^{p} : P \times IN_{+}^{|P|} \to IN_{+} \cup \{\infty\}$ is the capacity bound of each place, which can contain an *integer* number of *tokens*; $M_0$ is the initial marking; $\widetilde{\Lambda} : E_\tau \times IN_{+}^{|P|} \to IR^{+}$ is the function that determines the fuzzy firing rate $0 < \widetilde{\lambda}(e, M) < +\infty$ of timed event $e \in E_\tau$, that is *enabled* by the current marking $M$; $\widetilde{\omega} : E_0 \times IN_{+}^{|P|} \to IR^{+}$ is the fuzzy weight function $0 \le \omega(e, M) < +\infty$ which determines the firing fuzzy probability $\widetilde{q}(t, M)$ of immediate event $e \in E_0$, therein describe an probabilistic selector; $\widetilde{\rho} : P \cup E \to IR^{+}$ is the function that determines the fuzzy *reward rates* (real numbers) assigned to each current marking $M$ and to each firing event $e \in E$; $Lib_R$ (resp. $Lib_{At}$) is the set of $R\Gamma_v \in Lib_R$, (resp. $Atr_l \in Lib_{At}$,) *subnets* (resp. attributes) pattern class library involved in *structural reconfiguration* of the current $\Gamma FR$ by firing of an

enabled rewriting rule $r \in R$. In $\Gamma FR$ and $R\Gamma_v \in Lib_R$ nets the *quantitative attributes* can be specified as dependent on the current marking of the configured nets. Also, by default: $K^p(p_i)$ is unlimited and $g_e^E(M) = g_r^R(M) := True$.

In $\Gamma FR$ models, the attributes of net elements (arc cardinalities, places capacities, guard functions and event priorities, rewriting rules, firing rates, etc.) are matrix of the specified $z$ type that are defined by a set of matrix $A^z = [a_{ij}^z(s)]_{k \times n} \in \mathbf{A}$. The quantitative values attributes may be constant or marking-dependent functions of the specified type. The current activated element $a_{ij}^z(s)$ is specified by a set $P_A^z \subset P$ of net *control places*. For example, for the selection of current elements position in $A^z$, two control places should be specified. Therefore, the current number of tokens $i = m_l = M(p_l)$ and $j = m_v = M(p_v)$ in control places $p_l$ and $p_v$ shows the *position* of the respective element of $A^z$, and its values must be *imported* and taken into account when executing and analyzing the model [13].

Graphically, a matrix attribute of $\Gamma FR$ will be presented in a way that it will contain the matrix name in square brackets, i.e. $[A^z]$ (for details see Figure 3).

Figure 1 summarizes the graphical representation of FMRSRN structural elements features.

*Enabling and firing rules of events* $e \in E$ *by current marking* $M$ in $\Gamma FR$ are the same as for MRSRN [12, 13].

We only note that the dynamic reconfiguration of current $\Gamma FR$ by firing of enabled $r \in R$, if $g_r^R(M) := True$ is a map $r := \{RN_L, Atr_L\} \triangleright \{RN_W, Atr_W\}$, where $\{RN_L \in Lsp_{RN}, Atr_L \in Lsp_{Atr}\}$ (resp. $\{RN_W \in Lsp_{RN}, Atr_W \in Lsp_{Atr}\}$ is the *left-hand* (resp. *right-hand*) side of the binary *rewriting operator* $\triangleright$ assigned to $r \in R$, respectively. The execution of $\triangleright$ produce a *structural change* and/or *of attributes* in current $\Gamma FR'$ by replacing (*rewriting*) the specified subnet $\{RN_L, Atr_L\} \subseteq \Gamma FR'$ ($RN_L$ and $Atr_L$ are deleted) and a new $\{RN_W, Atr_W\} \in Lib_R$ are added belongs to the new resulting $\Gamma FR'' = (\Gamma FR' \setminus RN_L) \cup RN_W$ net, where the meaning of \ (and $\cup$) is *operation of removing* (resp. *adding*) $RN_L$ (resp. $RN_W$) *from* (resp. *to*) $\Gamma FR'$ (resp. $\Gamma FR' \setminus RN_L$). The places, events and arcs, which have the same names, that belong to $RN_W$ and $\Gamma FR' \setminus RN_L$ are *fused*, respectively [12].

But, if $g_r^R(M) := False$ then only the current $M$ marking will change to another $M'$ marking, i.e. $M[r > M'$ and the structure of $\Gamma FR'$ remains the same.

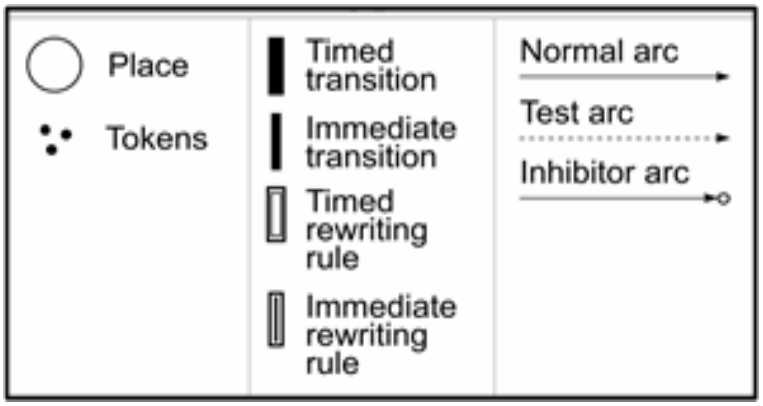



**Figure 1.** The structural elements features of $\Gamma FR$ models.

But, if $g_r^R(M) := False$ then only the current $M$ marking will change to another $M'$ marking, i.e. $M[r > M'$ and the structure of $\Gamma FR'$ remains the same.

## 3. Performability modeling case study

### A. *Informal Description of Attacked CBHS*

In this section, we will demonstrate the application of the FMRSRN for performability modeling of a particular CBHS1. For this one, we will consider the cloud biomedical healthcare system to be subject to intrusion-based attacks, where the attacker or intruder must first discover the vulnerabilities of this target system to perform the attack, being identified as the *attack surface*. In this case, the intruder will select the target node of the CBHS1 and try to identify vulnerabilities in its network (*reconnaissance stage*), then, if successful, he will create a remote access weapon (malware, such as a virus or worm) depending on the discovered vulnerabilities, it will transmit the weapon to the target through some means: USB drives; email attachments; websites, etc. (*delivery stage*). In this way, the malware starts working by acting on the target VM to exploit the vulnerability through: program code triggers (*exploit stage*); installing an access point for the intruder (*installation stage*); persistent access and control of the target VM (*command and control*); performing attacks such as exfiltrating or destroying data, encrypting for ransom, and so on (*target actions stage*).

Biomedical services are running on a CBHS1 platform, composed of ***n*** nodes (VMs), can randomly migrate between nodes according to a migration based MTD technique, triggered by a *timer* with a probabilistic or deterministic time period. As a result, the service may migrate to another node, but the attacker may remain on the same node. Also, we consider that the attacker adopts a try-and-error approach. Thus, the probability of a successful attack increases as long as the attacker remains within a certain physical machine pool. We will approximate this increasing probability with the FRSRN subnets that describe the $k$-phase *Cox* (resp. *hypoexponential* or *Erlang*) distribution of the attack time periods.

### B. *FMRSRN Security Model of CBHS Under MTD*

Figure 2 shows the proposed FMRSRN model, denoted $\Gamma FR1$, which describes the behavior of the attacker and the defender of CBHS1 using *time-based* MTD strategies [10, 11], that give a compact structural representation and at the same time to address the problem of state space explosion [9].

*The places, transitions and rewriting rules description* (*meaning*) *of* $\Gamma FR1$ *model are*:

- **Places.** $p1$ - attacker selected of the target node; $p2$ -intruder has access to the target node, after injecting a malware and then activating it, i. e. the exploit stage; $p3$- intruder's malware tries to attack the system through various methods; $p4$- attack success, the intruder acting on the data (exfiltration, corruption, etc.); $p5$- attacker is on the node where the service is running; $p6$ - intruder attack on one of the remaining (*n*–1) nodes without ser-vice; $p7$- time migration to each other different (*n* –1) nodes; $p8$- normal operating condition of a service; $p9$- start migration latency; $p14$ - potential task numbers to be processed; $p15$- tasks waiting queue to be processed; $p16$- one current task is in serving process (execution); $p17$- current service node is not busy.

• **Timed transitions.** $t3$ - period of time during which the attacker will perform desired actions; $t4$ - intruder abandon the current attack and sets another target node; $t5$ - attack time; $t6$ - timer with time interval between submitting node migration requests to the environment; $t7$ - migration time; $t19$ - service time of current task.

• **Immediate transitions.** $t8$ - migration of the ser-vice to a on one of $(N-2)$ *safe* nodes; $t9$ - migration of the service to a nod under attack; $t10$ - restart of timer; $t18$ - start of task service process. The firing of transition $t9$, with $q(t9,M)=1/(n-1)$ probability, leads to the migration of the service to a node under attack or on one of $(n-2)$ *safe* nodes by firing of $t8$ with the probability $q(t8,M)=(n-2)/(n-1)$. In these two cases, after the service is migrated, the timer starts again.

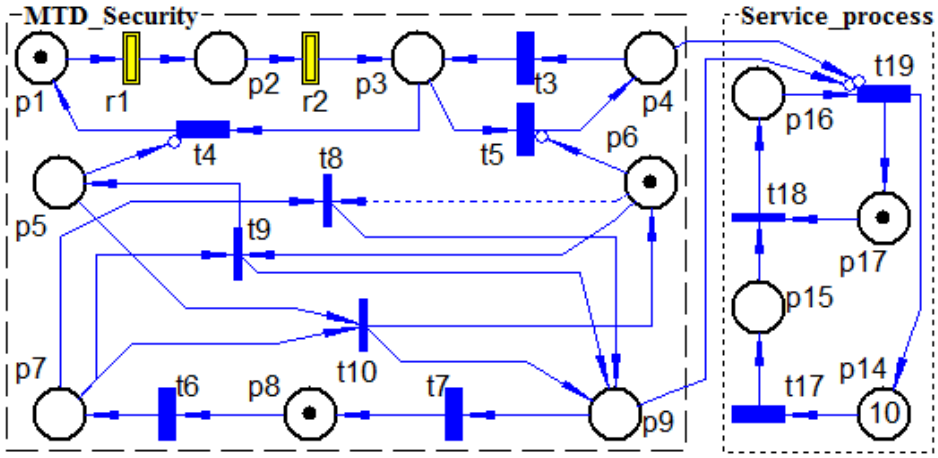



**Figure 2.** The $\Gamma FR1$ performability model of an CBHS1.

• **Timed rewriting rules.** $r1$ (resp. $r2$) – substitution of $t5$ by the $\Gamma cox-k\_t5$ subnet of Fig. 3a (resp. $\Gamma hypo\exp-k\_t5$) subnet of Fig. 3b) after the expiration of the time period that indicate the mean time required to *exploit* (resp. to *infect* ) a target node. The *firing* of $r1$, $r2$ in $\Gamma FR1$ occurs if intruder has access to the target node, after injecting a malware and: $g^E(r_2):=(M(p2)=1)$, $g^G(r_1):="True"$ and $g^G(r_2):="False"$.

A dynamic reconfiguration of $\Gamma FR1$ by the firing of enabled $r1$ is a map:

$r_1:=\{t5,\ g^G(r_1):="True"\}\triangleright\{g^G(r_1):="False",\Gamma cox-k\_t5\}$ or $r_1:=\{t5,\ g^G(r_1):="True"\}\triangleright\{g^G(r_1):="False",\Gamma hypo\exp-k\_t5\}$.

The rewriting operator $\triangleright$ represents a binary operation which produces a *structural change* in $\Gamma FR1$ by *replacing* the current subnet $R\Gamma_L\subseteq\Gamma FR1$ ($R\Gamma_L$ is removed) and a new $R\Gamma_j^w\in Lib_R$ subnet is *added* and *belongs* to the *new modified resulting net* $\Gamma FR1'=(\Gamma FR1\setminus R\Gamma_L)\cup R\Gamma_j^w$, where the meaning of **** (resp. $\cup$) is operation of *removing* (resp. *adding*) $RN_L$ *from* ($R\Gamma_j^w$ *to*) $\Gamma FR1$. **As example, i**n our case $R\Gamma_L:=\{t5,\ g^G(r_1):="True"\}$. For more detail to using of the rewriting rule $\triangleright$ operator see [12].

Note that when the firing of enabled $r1$ this rewriting rule will only change the current marking of $\Gamma FR1$, because $g^G(r_2):="False"$. If $g^G(r_2):="True"$ it is necessary to specify the $\triangleright$ operator with the corresponding subnets, i.e. $r_2:=\{R\Gamma_L\}\triangleright\{R\Gamma_j^w\}$.

*The places and transitions meaning of* $\Gamma cox-k\_t5$ (resp. $\Gamma hypo\exp-k\_t5$) *subnet are:*

• **Places.** $p10$ - current number of phases what must be executed; $p11$- finishing the execution of a current phase; $p12$ - allowing time period execution with phase-type distribution; $p13$- completion of the phase-type time period; $p14$-memory of the executed phase (current attack progress).

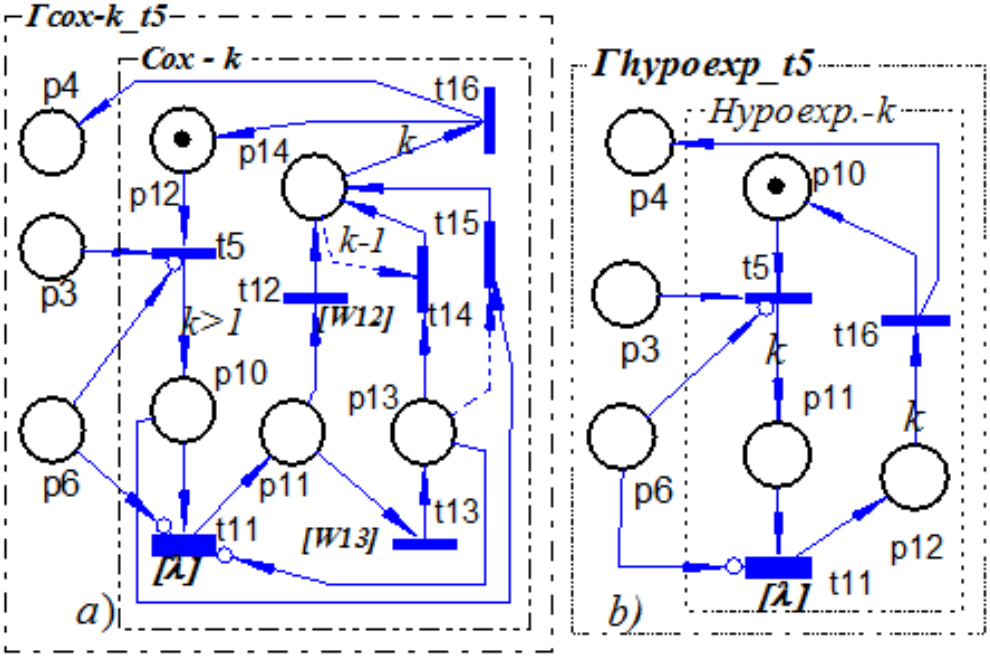



**Figure 3.** The $\Gamma_{FR1}$ subnets: a) $\Gamma cox-k\_t5$ ; b) $\Gamma hypo\exp-k\_t5$

• **Timed transitions.** $t11$- processing the current phases time with a selected $\lambda_{11,j} \in [\lambda]$ , $j=1,2,\ldots,k$ rate, where $[\lambda]$ is a matrix.

• **Immediate transitions.** $t5$ - start execution of the time period with the respective phase type distribution; $t12$ - selecting the next processing phase with probability $q_{12,j}$, $(j=1,2,\ldots,k)$, determined by the weight $w_{12,j} \in [W12]$, where $[W12]$ is a matrix; $t13$ - firing with probability $q_{13,j}$, $(j=1,2,\ldots,k-1)$, determined by the weight $w_{13,j} \in [W13]$, indicates that the attack time period is over after the execution of phase $j$. The $[W12]$ is a matrix; $t14$ and $t15$ - are used for reset of phase distribution time-out; $t16$ - denotes that the attacker successfully compromised target node.

The $k$ number of phases in these sub-nets (see Figure 3) is determined by the weights of respective arcs: $(t5, p10)$, $(p12, t16)$, $(t5, p10)$, $(p14, t14)$ and $(p14, t16)$.

Note that at *firing* of rewriting rule $r1$ in $\Gamma_{FR1}$ the places $p3, p4$ and $p6$ of $\Gamma_{FR1}$ net and $\Gamma cox-k\_t5$ (resp. $\Gamma hypo\exp-k\_t5$) subnet, that have the same name, will merge accordingly.

### *C. **Performability Analysis Case Study***

Performability analysis of $\Gamma_{FR1}$ model can be done following the approach described in [10-12]. The $\Gamma_{FR1}$ model is *bounded*, *live* and *reversible* [9], therefore there it exists a stationary behavior regime of the analyzed CBHS1.

Next, we will present a numerical case study of $\Gamma_{FR1}$ that show an application of the proposed approach. In this context, we will consider a particular case where the $t7$ timed

transition is an immediate transition, and the number of phases in the $\Gamma cox-k\_t5$ subnet is equal to 2.

We adopt an exponentially firing delay of all timed transitions with mean value $\bar{\tau}_i = 1/\lambda_i$ *hours*.

For the numerical evaluation of some performability metrics, based on parameter values taken from Chen et al. [14] parameters, we have used the VPNP tool [15].

Next, due to space constraint, we evaluate the impacts of $\lambda_6$ , $\tilde{\lambda}_{r1}$ and $n$ parameters on average availability and average throughput based on the $\Gamma FR1$ model.

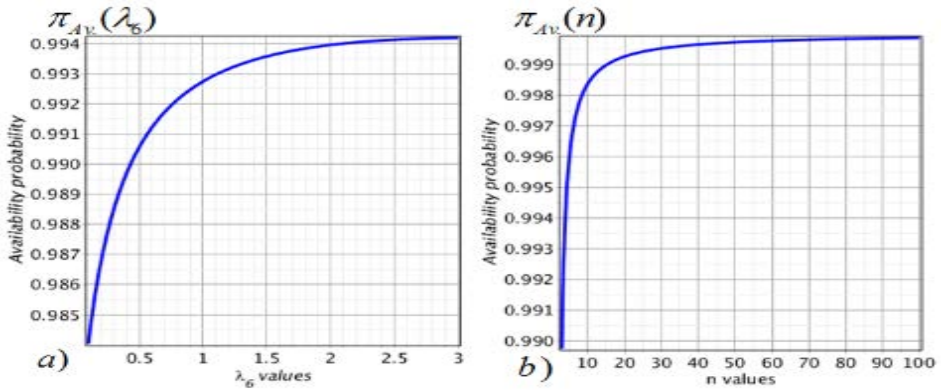
System availability is the $\pi_{Av.}$ probability that no token will be present in the $p4$ and/or $p9$ places, i.e. that the service of system is secure: $\pi_{Av.} = \Pr(M(p4)=0 \vee M(p9)=0) = 1-\pi_{Suc.}$, where $\pi_{Suc.} = \Pr(M(p4)=1 \vee M(p9)=1))$ is the attack success probability.

We compute the $\pi_{Av.}(\lambda_6)$ an $\pi_{Av.}(n)$ metrics of $MTD\_Security$ model depending on the $\lambda_6$ and $n$ parameters. For this, we use the following crisp values: firing delay of $t7$ is assumed to have a Cox-2 distribution with mean time hours $\bar{u}=2$ and the coefficient of variation $K^v=4$; the firing rates of timed transitions are: $\lambda_{r2}=1, \lambda_3=5, \lambda_4=8, \lambda_{11,1}=1, \lambda_{11,2}=0.125$ ; the firing probabilities of immediate transitions are: $q_{10}=(n-2)/(n-1), q_9=1/(n-1), q_{12}=0.25, q_{13}=0.75.$

As well, we consider two options: the first $\lambda_{r1}=0.04$ is a crisp value; the second case where this parameter has triangle fuzzy values, namely $\tilde{\lambda}_{r1}=(0.01, 0.04, 0.07).$

Figure 4a (resp. Figure 4b) shows the graphical representation of the $\pi_{Av.}(\lambda_6)$ (resp. $\pi_{Av.}(n)$) average availability variation, depending on the $\lambda_6$ (resp. $n$) parameter, for which $n=3$ (resp. $\lambda_6=3$) is considered a crisp value.

The computing result of $\pi_{Av.}(\lambda_6)$ (see Fig. 4a) for $\lambda_6=0.1$ (resp. $\lambda_6=2$) we obtain $\pi_{Av.}^{\min}(\lambda_6)=0.9841$ (resp. $\pi_{Av.}^{\max}(\lambda_6)=0.9946$). Also, the computing result of $\pi_{Av.}(n)$ (see Fig. 4b) for $n=3$ (resp. $n=100$) we obtain $\pi_{Av.}^{\min}(n)=0.9875$ (resp. $\pi_{Av.}^{\max}(n)=0.9998$)




a) b)

**Figure 4.** Computing results for average availability probability $\pi_{Av.}$: a) $\pi_{Av.}$ depending of $\lambda_6$; b) $\pi_{Av.}$ depending of *n*.

Similarly, we will evaluate the fuzzy average availability system variation, considering it to be a function that depends on the parameters $\lambda_6$ and $\tilde{\lambda}_{r1}$. This metric, denoted $\tilde{\pi}_{Av.}(\lambda_6, \tilde{\lambda}_{r1})$, was

performed for the case: $n=3,\ \lambda_6 \in [0.1, 3]$ and $\tilde{\lambda}_{r1}=(0.01, 0.04, 0.07)$ is a triangle fuzzy number, and the other parameters have values that were considered in the previous case.

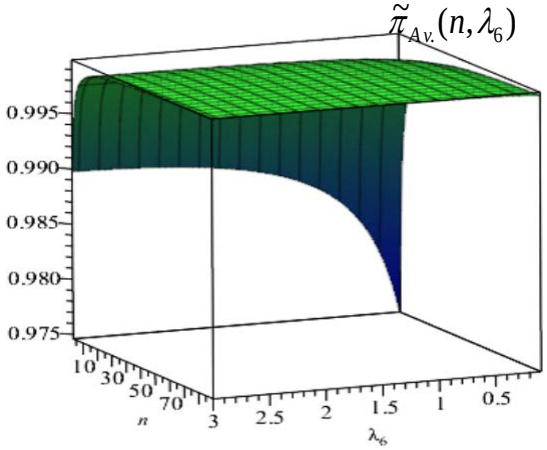



**Figure 5.** The evolution of $\pi_{Av.}$ function depending of $n$ and $\lambda_6$ values.

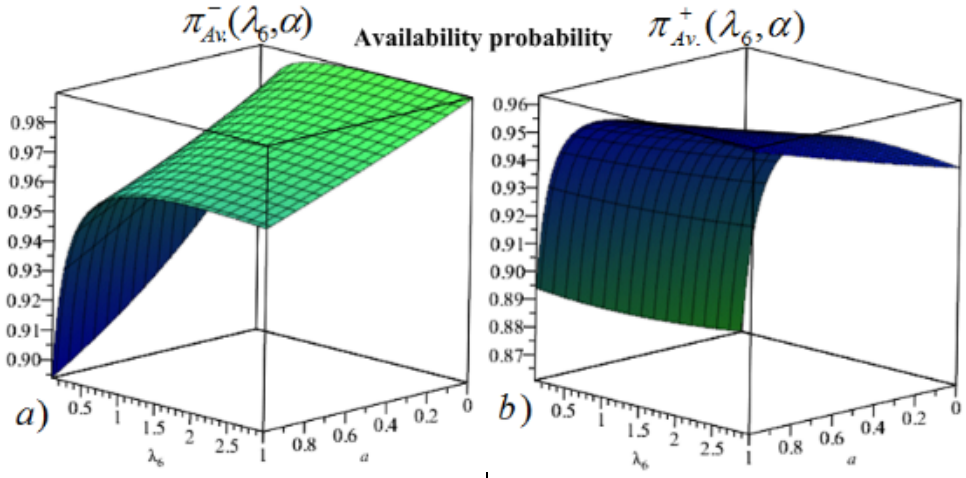
Expressed $\tilde{\lambda}_{r1}$ in terms of $\alpha-cut$ we have [10]: $\tilde{\lambda}_{r1}(\alpha)=[0.04-0.03\cdot(1-\alpha),\ 0.04+0.03\cdot(1-\alpha)]$.

For these $\tilde{\lambda}_{r1}(\alpha)$ fuzzy parameters, the evaluation of $\tilde{\pi}_{Av.}(\lambda_6,\alpha)=[\pi^{-}_{Av.}(\lambda_6,\alpha),\pi^{+}_{Av.}(\lambda_6,\alpha)]$ in $\alpha-cut$ are obtained based on the methods presented in [10].

Since $\forall\, 0<\tilde{\pi}_i(\alpha)<1$, therefore the $\tilde{\lambda}_{r1}(\alpha)$ is applicable to the $0\le\alpha\le1$ interval. Thus, we can perform the variation of $\tilde{\pi}_{Av.}(\lambda_6,\alpha)=[\pi^{-}_{Av.}(\lambda_6,\alpha),\ \pi^{+}_{Av.}(\lambda_6,\alpha))$ that depends of the $\lambda_6$ and $\alpha$ crisp values.

In the same context, Figure 5 plots the evolution results of $\pi_{Av.}(n,\lambda_6)$ that depend on the simultaneous variation of the $n$ and $\lambda_6$ values.

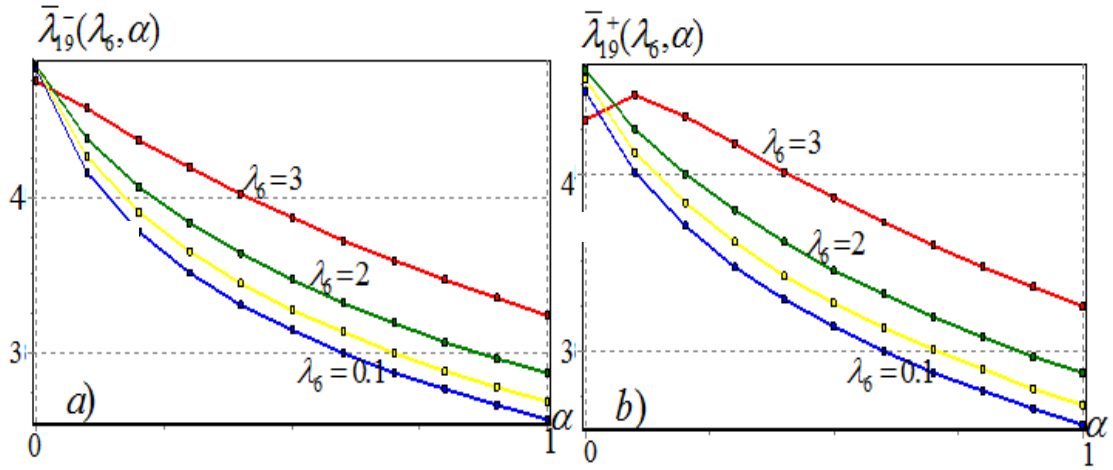
Also, Figure 6 displays the $\tilde{\lambda}_{19}(\lambda_6,\alpha)$ fuzzy *average availability* probability variation, depending of the $\lambda_6$ and $\alpha$ *-cut*, respectively. Thus, for $\lambda_6=2$ it is obtained: $[\pi^{-}_{Av.}(\lambda_6,0)=0.9899,\ \pi^{+}_{Av.}(\lambda_6,0)=0.8939]$; $\pi^{-}_{Av.}(\lambda_6,1)=\pi^{+}_{Av.}(\lambda_6,1)=0.9632$




a) | b)

**Figure 6.** The fuzzy average availability variation:
a) $\pi^{-}_{Av.}$ depending of $\lambda_6$ and $\alpha-cut$; b) b)$\pi^{+}_{Av.}$ depending of of $\lambda_6$ and $\alpha-cut$.

Figure 7 depicts how the impact of the uncertainty on the $\lambda_{r1}$ rate and variation value of $\lambda_6$ rate affects the $\tilde{\lambda}_{19}(\lambda_6,\alpha)$ fuzzy *throughput* of CBHS1 that measure of how many tasks can be processed in a given amount of time.




a) b)

**Figure 7.** The fuzzy throughput of CBHS1: a) $\bar{\lambda}_{19}^{-}$ *d*epending of $\lambda_6$ and $\alpha-cut$; b) $\bar{\lambda}_{19}^{+}$ depending of of $\lambda_6$ and $\alpha-cut$.

For the case that $\lambda_6=3$ and $\lambda_{19}=5$ it is obtained: $\tilde{\lambda}_{19}(\lambda_6,0)=[\bar{\lambda}_{19}^{-}(\lambda_6,0)=4.8270,\ \bar{\lambda}_{19}^{-}(\lambda_6,0)=4.4660\ ]$;

$\tilde{\lambda}_{19}(\lambda_6,1)=[\ \bar{\lambda}_{19}^{-}(\lambda_6,1)=2.5800,\ \ \bar{\lambda}_{19}^{+}(\lambda_6,0)=2.5800\ ].$

## 4. Conclusions

The proposed in this article modeling approach based on Matrix Rewriting Stochastic Reward Nets with Fuzzy parameters is highly scalable, flexible and customizable through several crisp and fuzzy parameters. It also allows to stochastically characterize the underlying behaviors and phenomena with epistemic uncertainties through phase type distributions, obtaining steady-state average availability and performance metrics of CBHSs with other practical D techniques.

As future work, we plan to investigate the *trade-offs* between security, availability, cost and performance of CBHSs when different MTD techniques are applied. Also, we will focus on developing a software system incorporate into VPNP Tool with a friendly interface for checking behavioral properties and performability analysis of FMRSRN models.

This research was conducted within the LifeTech project at the Technical University of Moldova, the results were presented in the Biomedical Section of the 13th International Conference on Electronics, Communications, and Computing (IC ECCO-2024), organized by the Technical University of Moldova, held in Chișinău, Moldova, on October 17–18, 2024.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**


1. Guo, B.; Shukor, N.S. A.; Ishak, I.S. Enhancing healthcare services through cloud service: a systematic review. *International Journal of Electrical & Computer Engineering* 2024, 14(1), pp. 1135–1146.
2. Mathkor, D.M.; Mathkor, N.; Bassfar, Z.; Bantun, F.; Slama, P.; Ahmad, F.; Haque, S. Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. *Journal of infection and public health* 2024 17(4), pp. 559-572.
3. Aijaz, M.; Nazir, M.; Mohammad, M. Threat Modeling and Assessment Methods in the Healthcare-IT System: A Critical Review and Systematic Evaluation. *SN Computer Science* 2023, 4, 714.
4. Luna, R.; Rhine, E.; Myhra, M.; Sullivan, R.; Kruse, C.S. Cyber threats to health information systems: A systematic review. *Technology and Health Care* 2016, 24(1), pp. 1-9.
5. Nguyen, T.A.; Fe, I.; Brito, C.; Kaliappan, V.K.; Choi, E.; Min, D.; Silva, F.A. Performability evaluation of load balancing and fail-over strategies for medical information systems with edge/fog computing using stochastic reward nets. *Sensors* 2021, 21(18), 6253.
6. Zheng, J.; Namin, A.S. A survey on the moving target defense strategies: An architectural perspective. *Journal of Computer Science and Technology* 2019, 34(1), pp. 207–233.
7. Sun, R.; Zhu, Y.; Fei, J.; Chen, X. A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive. *Applied Sciences* 2023, 13(9), 5367.
8. Distefano, S.; Scarpa, M.; Chang, X.; Bobbio, A. Assessing dependability of web services under moving target defense techniques. In: *Proceedings of the 30th European Safety and Reliability Conference*, 2020, pp. 1988-1995.
9. Muppala, J.; Ciardo, G.; Trivedi, K.S. Stochastic reward nets for reliability prediction. *Commun. Reliab. Maintainab. Serv.* 1994, 1(2), pp. 9–20.
10. Tuysuz, F., Kahraman, C. Modeling a flexible manufacturing cell using stochastic Petri nets with fuzzy parameters. *Expert Systems with Applications* 2010, 37, pp. 3910–3920.
11. Philip, A.; Sharma, R.K. A stochastic reward net approach for reliability analysis of a flexible manufacturing module. *Int J Syst Assur Eng Manag* 2013, 4, pp. 293–302.
12. Moraru, V.; Guţuleac, E.; Zaporojan, S. Uncertainty modelling of dynamically reconfigurable systems based on rewriting stochastic reward nets with z-fuzzy parameters. *Computer Science Journal of Moldova* 2021, 29, 3(87), pp. 388-406.
13. Guţuleac, E.; Zaporojan, S.; Gîrleanu, I.; Cărbune, V. Hybrid stochastic Petri nets with matrix attributes for modelling of discrete-continuous process. *Meridian Ingineresc* 2016, 2, pp. 34–40.
14. Chen, Z.; Chang, X.; Han, Z.; Yang, Y. Numerical evaluation of job finish time under MTD environment, *IEEE Access* 2020, 8, pp. 413–416.
15. Guţuleac, E.; Boşneaga, C.; Reilean, A. VPNP-Software tool for modeling and performance evaluation using generalized stochastic tri nets. In: *Proc. of 6-th International Conference on D&AS-2002*, Suceava, Romania, 2002, pp. 243-248.


**Citation:** Moraru, V.; Sclifos, A.; Cuzmin, S.; Guţuleac, E. Analysis of cloud biomedical healthcare systems security based on matrix rewriting SRNS with fuzzy parameters. *Journal of Engineering Science*. 2025, XXXII (3), pp. 64-74. https://doi.org/10.52326/jes.utm.2025.32(3).06.



**Submission of manuscripts**: jes@meridian.utm.md