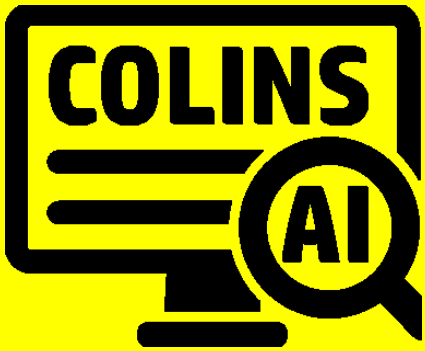
Vasyl Lytvyn
Natalia Sharonova
Izabela Jonek-Kowalska
Agnieszka Kowalska-Styczen
Victoria Vysotska
Yevhen Kupriianov
Olga Kanishcheva
Olga Cherednichenko
Thierry Hamon
Natalia Grabar
(Eds.)



COMPUTATIONAL LINGUISTICS AND INTELLIGENT SYSTEMS

Proceedings of the 6th International Conference, COLINS-2022.
Volume I: Main Conference

Gliwice, Poland
May, 2022, 12-13

Models for Cloud System Availability Assessment Considering Attacks on CDN and ML Based Parametrization

Yuriy Ponochovnyi [1], Oleg Ivanchenko [2], Vyacheslav Kharchenko [3], Iryna Udovyk [2] and Eduard Baiev [4]

[1] *Poltava State Agrarian University, 1/3, Skovorody str., Poltava, 36003, Ukraine*
[2] *Dnipro University of Technology, Dmytra Yavornytskogo Ave. 19, Dnipro, 49005, Ukraine*
[3] *National Aerospace University "Kharkiv Aviation Institute", 17, Chkalova str., Kharkiv, 61000, Ukraine*
[4] *Yalantis, bul. Slavy, 56, Dnipro, 49156, Ukraine*

Abstract

The article proposes a method for assessing the availability of the cloud system taking into account the variable dynamics of attacks on vulnerabilities Content Delivery Network (CDN). The architecture of the cloud system for video hosting services is detailed, on the basis of which an example of simulation in the conditions of cyberattacks, software and hardware failures is given. An availability model based on the Reliability Block Diagram (RBD), a Markov model (MMC) with constant parameters of failure and recovery rates, and a multifragment (MFM) model with a variable parameter that estimates the probability of attacks have been developed and studied. Two scenarios of events that affect the availability of the system are considered: the first - in the absence of attacks on the CDN component; the second - in attacks that cause an increase in the CDN failure rate to the limit level. A comparative analysis of RBD, MMC and MFM and assessment of discrepancies in the simulation results were performed. The use of Big Data analytics and ML tools is proposed for parametrization of models. The obtained simulation results can be used not only by users of cloud systems, but also by Cloud Service Providers (CSP) to improve planning procedures and risk assessment of failures.

Keywords

Availability assessment, multifragment markov models, cloud system, reliability block diagrams, attack on content delivery network, machine learning for model parametrization

1. Introduction

Modern technological developments have increased the need to use web technologies, which, in particular, as a computer paradigm with the appropriate capabilities: greater flexibility and affordability at a low cost. Effective implementation of modern information technologies: Web, Cloud, IoT (Internet of Things), etc. it is impossible without the corresponding normative documents describing legal norms, problems, risks and ways of their minimization. Convenient and secure use of web and Cloud services is based on the principles of trust between service providers and users, but trust is not possible without the support and provision of service level agreements (SLAs). Another factor in guaranteeing such trust is the comprehensive provision of regulatory standards at the international and national levels.

Demand for cloud computing is growing every year due to their key characteristics, which have been most comprehensively and fundamentally described by the European Union Agency for Cyber Security (ENISA) [1] and the National Institute of Standards and Technology (NIST) [2]. However, the use of cloud technologies alone does not minimize the risks of accidents, catastrophes, cyberattacks and component failures, which is especially important for critical infrastructure. To minimize such risks, it

COLINS-2022: 6th International Conference on Computational Linguistics and Intelligent Systems, May 12–13, 2022, Gliwice, Poland
EMAIL: yuriy.ponch@gmail.com (Y. Ponochovnyi); ivanchenko.o.v@nmu.one (O. Ivanchenko); v.kharchenko@csn.khai.edu (V. Kharchenko); udovyk.i.m@nmu.one (I. Udovyk); edbaev@gmail.com (E. Baiev)
ORCID: 0000-0002-6856-2013 (Y. Ponochovnyi); 0000-0002-5921-5757 (O. Ivanchenko); 0000-0001-5352-077X (V. Kharchenko); 0000-0002-5190-841X (I. Udovyk); 0000-0002-6707-3170 (E. Baiev)

is necessary to maintain not only the support and counteracting system, but to close the foundations of fault tolerance, availability and resistance in the early stages of planning and design. That is why the development of a methodology for the development and maintenance of cloud systems of high availability for critical infrastructure is an urgent issue.

Currently, the industrial provision of services provided by various cloud service providers (CSP) and among them the largest Amazon, Microsoft and Google [3]. CSPs provide users with flexible plans for renting and maintaining virtual cloud infrastructure and services based on IaaS, PaaS, SaaS and others. According to these user requirements for the availability of the cloud system and its elements, which are usually supported by simple model calculations (such as methods of the Reliability Block Diagram (RBD) or failure tree analysis (FTA)), various internal and external factors or the dynamics of their changes may not be taken into account. On the other hand, the use of a Markov [4] or semi-Markov [5] models should be justified, requiring time and computing resources. We propose to perform a comparative analysis of availability models of cloud architecture (on the example of a video hosting system). The paper considers a simple model based on RBD, a Markov model with constant parameters, and a Multifragment model with a variable parameter. The discrepancy of simulation results is estimated. The obtained simulation results can be used not only by users of cloud systems, but also by CSP service personnel to improve the planning and failure risk assessment procedure.

2. Related Works

The issue of assessing the quality of cloud services is relevant and widely covered in scientific works. When calculating the reliability and availability of most authors [6] use models based on RBD and failure trees [7]. The issues of calculating the input parameters for such models are covered in [8] (the assessment of the availability of the virtualized environment for different scenarios of their use). The study [9] also evaluated the input parameters for a specific pattern - the cloud mobile system.

Complex models based on the Markov approach have been considered in subsequent publications. In [10], the Stochastic Reward Nets was created. Works [11-12] contain queuing models and case, based on Markov reward models.

In [13] authors describe the approach based on the use of Semi-Markov models to assess availability of a cloud infrastructure with multiple pools. Unlike Markov, the Semi-Markov models are utilized by researchers when the system operated at diverse modes on different intervals in time.

In [14] the analysis of software failure data was performed in order to determine the optimal laws of time distribution between expected failures. The study [15] analyzed a sample of data on vulnerabilities of software servers based on an open repository [16]. Since these studies do not specify an analysis tool, it can be concluded that manual data processing was performed.

The approach proposed in this article has already been approved in a study [17], which compared the results of modeling Markov and semi-Markov models of cloud service. The research performed here is a logical continuation [17], as it was specified values of input parameters and results by using the Markov and Multifragment models.

3. Methodology

3.1. Approach and stages of modelling and assessment

Research methodology is based on the use of the principles of systems analysis [18-19] in setting and solving research problems. This is manifested in [18]:

- determining the stages of solving tasks and the logical sequence of their implementation;
- the choice of adequate mathematical apparatus, research methods and their correlation with the tasks of individual stages;
- formal presentation of types, procedures, indicators and parameters that describe the functioning of the cloud system and external influences on it;

- decomposition of the cloud system architecture into components and study of their relationships in the tasks of analysis, evaluation and ensuring availability;

- establishing and studying the relationship between the resulting indicators of cloud system availability, obtained using various mathematical models, taking into account the peculiarities of their operation, maintenance and use.

3.2. Architecture of system modelled: CVS

To model the processes that accompany the operation of the cloud architecture (failures and restored component systems, attacks on nah, installation of patches) was created cloud architecture model. The cloud system is a complex multilevel and distributed system that can be represented by a diagram of different levels of nesting [8,10]. The cloud architecture model describes a three-level client-server network architecture that includes three networks (mobile, CDN and primary virtual network) to service groups of end devices.

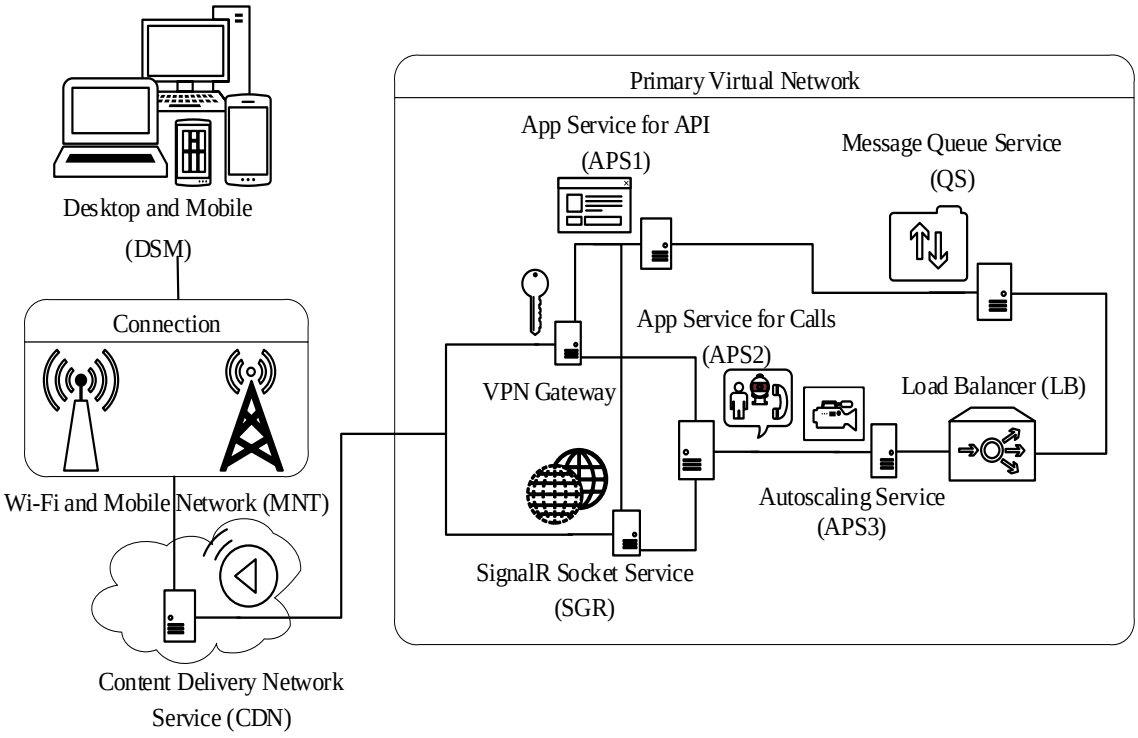


Figure 1: Architecture of CVS

The paper considers an example of the functioning of cloud services for video traffic processing. The CDN is separated from the Primary Virtual Network by the SignalR Socket Service and the VPN Gateway, as shown in Figure 1. Application services (App Service API, Calls and Autoscaling Service) are hosted on the Primary Virtual Network. The Virtual Network also uses the Message Queue Service (QS) and Load Balancer (LB).

Thus, the common elements for a typical cloud system are a group of end devices (DSM), a physical access network (MNT), elements of a virtual access network (VPN and SGR) and load balancing (LB). Cloud application services (API, Calls, Autoscaling) are special for video hosting services. An important element, such as CDN, should be singled out, as the use of such a network allows in part unload regional cloud services. CDN also provides protection against DDoS-type cyberattacks, but this element is the most accessible for criminal activities.

4. Availability models

4.1. RBD availability model

The failure of any unreserved element of the cloud system architecture (Figure 1) will cause unavailability in customer service. Based on this, the Reliability Block Diagram (RBD) of the cloud system (Figure 2) will include seven consecutive elements, each of which characterizes the serviceability of the corresponding elements of the architecture. Elements of architecture: WiFi and MNT, SGR and VPN form parallel links in RBD. The developed model does not describe redundant service configuration, but both web servers (LB, QS) and application servers (APS) can be reserved through a high availability cluster, in which case RBD will contain additional redundant components.

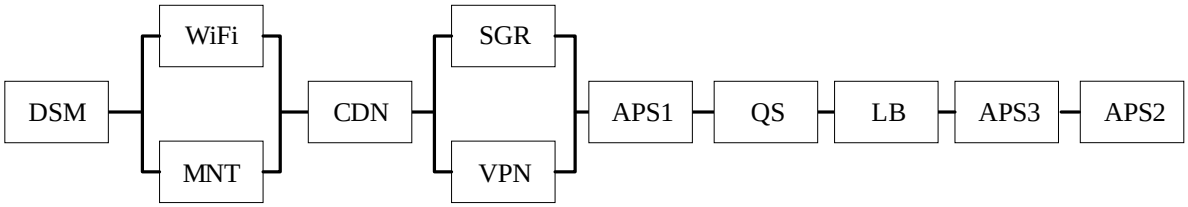


Figure 2: RBD for CVS

Also developed RBD can be detailed, because each service is primarily implemented as a client-server distributed structure (respectively, it is characterized by failures and restores the client and server page) [10]. Secondly, services are created on the basis of hardware and software systems (respectively, they are characterized by failures of hardware and software) [12]. However, in the developed model it was decided to limit certain values of failures due to physical and design defects and attacks on the vulnerability of the component.

According to the method, as recommended in [4], the calculation of the availability of the system with a mixed connection of elements is performed by formula (1)

$$A_{CVS} = A_{DSM} \times A_{CDN} \times A_{WM} \times A_{APS1} \times A_{QS} \times A_{LB} \times A_{APS3} \times A_{APS2}\,, \quad (1)$$

where

$$A_{WM} = 1-(1-A_{Wi-Fi})(1-A_{MNT})\,,\ A_{VS} = 1-(1-A_{VPN})(1-A_{SGR})\,. \quad (2)$$

The availability values obtained by formulas (1) and (2) are stationary. This greatly simplifies the model, but does not allow to study the dynamics of changes in availability function over time.

4.2. Markov availability model

The graph of states and transitions of the Markov model of the cloud system (Figure 3) includes one serviceable state S1, four operational states S4, S6, S10, S12 and nine inoperable states S2, S3, S5, S7, S8, S9, S11, S13, S14. This Markov model describes the functioning of the cloud system in terms of manifestation of only hardware and software defects under the condition of averaging the failure rates and recovery of components of the architecture, performed on the basis of the method [4]. The model does not describe changes in the intensity of design defects (for example, during attacks on components). However, using repeated reproduction of the model experiment, you can get the dynamics of changes in the resulting indicator when changing one or more input parameters.

The system of Kolmogorov-Chapman differential equations constructed for the graph of the model in Figure 3 is represented by formula (3).

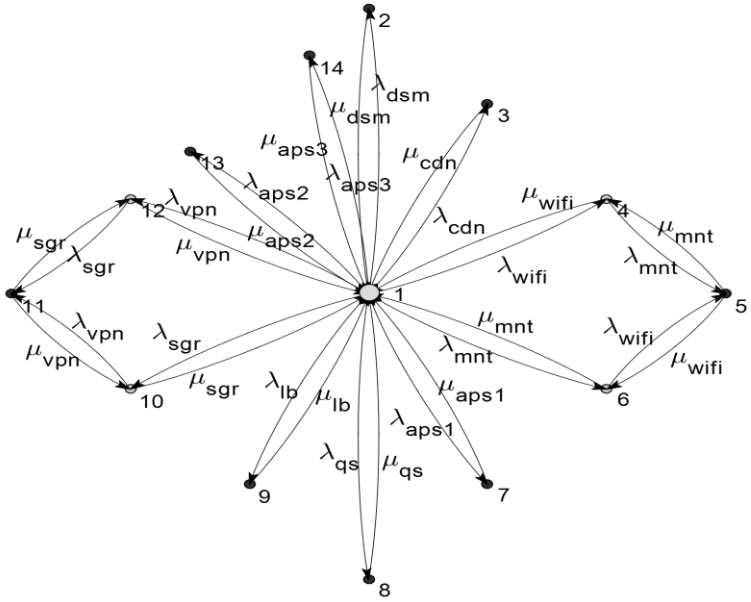


Figure 3: Digraph of the cloud system Markov model

$$
\begin{cases}
\frac{dP_1(t)}{dt} = -\left(\lambda_{DSM} + \lambda_{CDN} + \lambda_{Wi-Fi} + \lambda_{MNT} + \lambda_{APS1} + \lambda_{QS} + \lambda_{LB} + \lambda_{SGR} + \lambda_{VPN} + \lambda_{APS2} + \lambda_{APS3}\right) P_1(t) + \\
\quad + \mu_{DSM} P_2(t) + \mu_{CDN} P_3(t) + \mu_{Wi-Fi} P_4(t) + \mu_{MNT} P_6(t) + \mu_{APS1} P_7(t) + \mu_{QS} P_8(t) + \mu_{LB} P_9(t) + \\
\quad + \mu_{SGR} P_{10}(t) + \mu_{VPN} P_{12}(t) + \mu_{APS2} P_{13}(t) + \mu_{APS3} P_{14}(t); \\
\frac{dP_2(t)}{dt} = -\mu_{DSM} P_2(t) + \lambda_{DSM} P_1(t); \\
\frac{dP_3(t)}{dt} = -\mu_{CDN} P_3(t) + \lambda_{CDN} P_1(t); \\
\frac{dP_4(t)}{dt} = -\left(\mu_{Wi-Fi} + \lambda_{MNT}\right) P_4(t) + \lambda_{Wi-Fi} P_1(t) + \mu_{MNT} P_5(t); \\
\frac{dP_5(t)}{dt} = -\left(\mu_{Wi-Fi} + \mu_{MNT}\right) P_5(t) + \lambda_{Wi-Fi} P_4(t) + \lambda_{MNT} P_6(t); \\
\frac{dP_6(t)}{dt} = -\left(\lambda_{Wi-Fi} + \mu_{MNT}\right) P_6(t) + \lambda_{MNT} P_1(t) + \mu_{Wi-Fi} P_5(t); \\
\frac{dP_7(t)}{dt} = -\mu_{APS1} P_7(t) + \lambda_{APS1} P_1(t); \\
\frac{dP_8(t)}{dt} = -\mu_{QS} P_8(t) + \lambda_{QS} P_1(t); \\
\frac{dP_9(t)}{dt} = -\mu_{LB} P_9(t) + \lambda_{LB} P_1(t); \\
\frac{dP_{10}(t)}{dt} = -\left(\mu_{SGR} + \lambda_{VPN}\right) P_{10}(t) + \lambda_{SGR} P_1(t) + \mu_{VPN} P_{11}(t); \\
\frac{dP_{11}(t)}{dt} = -\left(\mu_{SGR} + \mu_{VPN}\right) P_{11}(t) + \lambda_{VPN} P_{10}(t) + \lambda_{SGR} P_{12}(t); \\
\frac{dP_{12}(t)}{dt} = -\left(\lambda_{SGR} + \mu_{VPN}\right) P_{12}(t) + \lambda_{VPN} P_1(t) + \mu_{SGR} P_{11}(t); \\
\frac{dP_{13}(t)}{dt} = -\mu_{APS2} P_{13}(t) + \lambda_{APS2} P_1(t); \\
\frac{dP_{14}(t)}{dt} = -\mu_{APS3} P_{14}(t) + \lambda_{APS3} P_1(t), \\
\sum_{i=1}^{14} P_i(t) = 1.
\end{cases}
\tag{3}
$$

$$P_1(0) = 1, \ \forall \ P_i(0) = 0, \text{ where } i = 2,3,...,14 \tag{4}$$

To obtain single solution to this system additions in the form of initial conditions were applied (4).

Modeling the change of the input parameter requires the introduction of an additional cycle, in which when changing the parameter each time the Markov model is recalculated. A code for such operations has the following form.

```
la_cdn_n = [0.001388889: 0.004027778: 0.041666667];
Ag=[]; P0=[1 zeros(1, size(V1,1)-1)];
for j=1:length(la_cdn_n)
    la_cdn = la_cdn_n(j);
    E1=[E1; 1 3 la_cdn]; A=matrixA(V1,E1);
    [t1,P1] = ode15s(@stiff, taim_interval,P0,options);
    Ag=[Ag P1(:,1)+P1(:,4)+P1(:,6)+P1(:,10)+P1(:,12)];
end;
```

In the given code fragment for storage of availability function values the array Ag is used, and the resulting indicator is defined by the formula (5).

$$A(t) = P_1(t) + P_4(t) + P_6(t) + P_{10}(t) + P_{12}(t) . \tag{5}$$

4.3. Multifragment availability model considering attacks on CDN

The multifragment model of cloud system availability allows taking into account the change of input parameters in one model step. This complicates the marked digraph of the functioning of the system, as shown in Fig.4. The process of functioning of the cloud system is as follows. Initially, the system implements all planned functions and is in state S1. In the process of functioning, the failures of the system components are manifested, as a result of which it passes into the state S2..S14 and is restored (the system returns to the state S1). To simplify the perception of the model, in digraph (Fig. 4) all transitions not related to the attack on the CDN are hidden in the superstates S(1..14 *) (for the first fragment) and S(15..28 *) (for the second fragment).

After a certain time interval, the system fails due to an attack on the vulnerability of the CDN component, and it goes into state S3. If the attacker succeeds (the CDN attack was successful), the system moves to a new part of the model (state S17), and if the attack fails, it returns to state S1. The probability of success of the attacker is weighted by the parameter a∈ [0..1]. After several successful attacks (usually Nf = [8..12], the intensity of the attack reaches its maximum (because for technical reasons, the attacker can not speed them up).

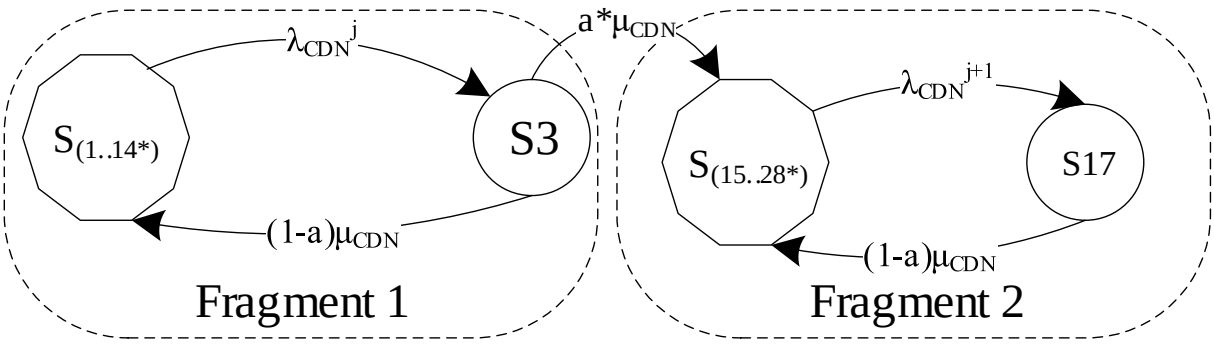


Figure 4: Orgraph of multifragment availability models CVS

The value of the resulting availability indicator in the multifragment model is determined by formula (6).

$$A(t) = \sum_{i=0}^{N_f - 1} \left[P_{14i+1}(t) + P_{14i+4}(t) + P_{14i+6}(t) + P_{14i+10}(t) + P_{14i+12}(t) \right]. \tag{6}$$

5. Results of modelling

5.1. Models assumptions and ML based parametrization

When building availability models of cloud system, the following assumptions were made [4,5].

a) For the RBD availability model:

- the availability of each of the components of the cloud architecture in equation (1) is determined by the formula $\mu_i/(\mu_i+\lambda_i)$, where the values of μ_i and λ_i are the input parameters averaged by method [4] for each element of the cloud system.

b) For the Markov model of the cloud system:

- the flow of events that translates the system from one functional state to another has the properties of stationary, ordinariness and absence of aftereffects, respectively, the input parameters of the model λi, μi are assumed to be constant;
- each element of the cloud system at any time may be in working order or inoperable states.

c) For the multifragment cloud system model:

– after elimination of CDN vulnerability in F1 fragment, the intensity of attack on CDN is specified as λ_{CDN}^{j+1}, and is defined as:

$$\lambda_{CDN}{}^{j+1} = \lambda_{CDN}{}^{j} + \Delta\lambda \,, \tag{7}$$

– the intensity of attack on CDN component (for technical reasons) is limited by the maximum λ_{CDN}^{max}.

Parametrization of input data for the proposed models was performed using Machine Learning tools [21]. In particular, utilized machine learning operations MLlib based on the use of Spark Big Data Platform were used [22]. Statistical processing and evaluation of data characterizing the reliability of the components of the cloud video system was implemented by sequentially performing operations to create Resilient Distributed Datasets, (RDD). In doing on, RDDs were formed from tuples of data that contained statistics on the reliability of CVS components. Next, the formed RDD datasets were transformed into matrix constructs, which were subjected to the operation of statistical testing of hypotheses (Hypothesis Testing) in accordance with the criterion of xi-square (Chi-square test). Figure 5 shows the solutions' scheme using operations of RDDs and Machine Learning.

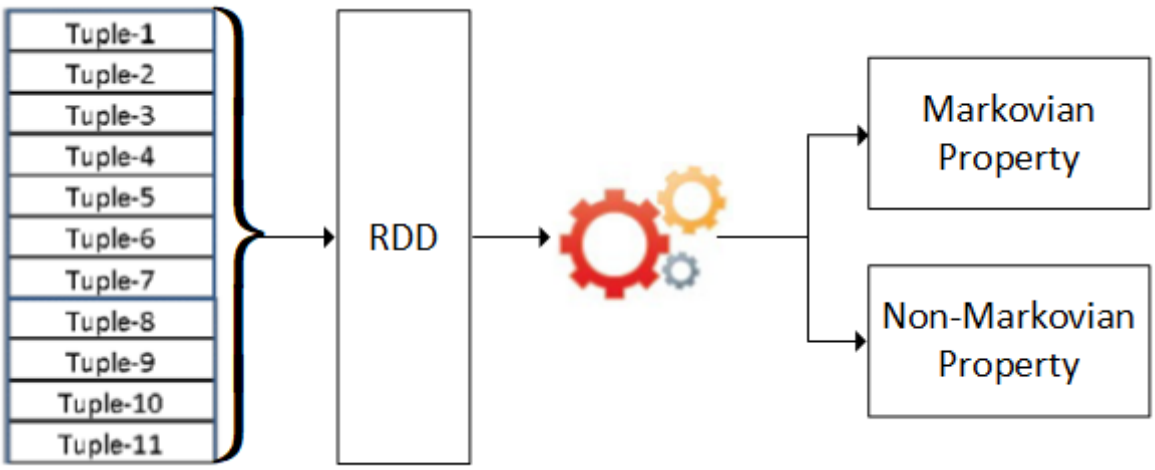


Figure 5: Solutions' scheme using operations of RDDs and Machine Learning

The primary input parameters of RBD, Markov and Multifragment models were determined on the basis of research and certification data [6,8,9] for the analog versions CVS samples. Their values are presented in Table 1.

Table 1
Constant values of simulation processing input parameters for RBD and Markov models

#	Name of Systems Components	Failure rate	Value (1/h)	Repair Rate	Value (1/h)
1	Desktop and Mobile (DSN)	la_dsm	0,000925926	mu_dsm	0,02083
2	Content Delivery Network Service (CDN)	la_cdn	0,001388889	mu_cdn	1
3	Wi-Fi	la_wifi	0,001488095	mu_wifi	0,04167
4	Mobile Network (MNT)	la_mnt	0,000462963	mu_mnt	0,5
5	App Service (API)	la_aps1	0,002083333	mu_aps1	1,5
6	Queue Service (QS)	la_qs	0,001302083	mu_qs	1
7	Load Balancer (LB)	la_lb	0,001190476	mu_lb	1
8	SignalR Socket Service (SGR)	la_sgr	0,001666667	mu_sgr	1
9	VPN Gateway	la_vpn	0,001736111	mu_vpn	1
10	App Service (Calls)	la_aps2	0,00245098	mu_aps2	0,66667
11	Autoscaling Service	la_aps3	0,002777778	mu_aps3	1

To study the availability of the system, variable values of the input parameter λ_{CDN}^{j} were adopted, which are substantiated in [11] and summarized in Table 2.

Table 2
Variable values of simulation processing input parameters for Multifragment model

#	Systems Name	Matlab variable	Value (1/h)
1	Minimum value of CDN failure rate due to hacker attack	la_cdn_min	0,001388889
2	Maximum value of CDN failure rate due to hacker attack	la_cdn_max	0,041666667
3	Delta of change CDN failure rate	delta_la_cdn	0,004027778
4	Probability of successful attack	alpha	0..1
5	Number of fragments in Multifragment model	nf	10

5.2. Simulation and comparative analysis

Comparison of RBD and Markov models is performed under the condition $t\to\infty$ (for stable Availability). Under this condition, the solution of the Markov model is reduced to a system of linear (non-differential) equations. The results of the calculations are shown in Table 3.

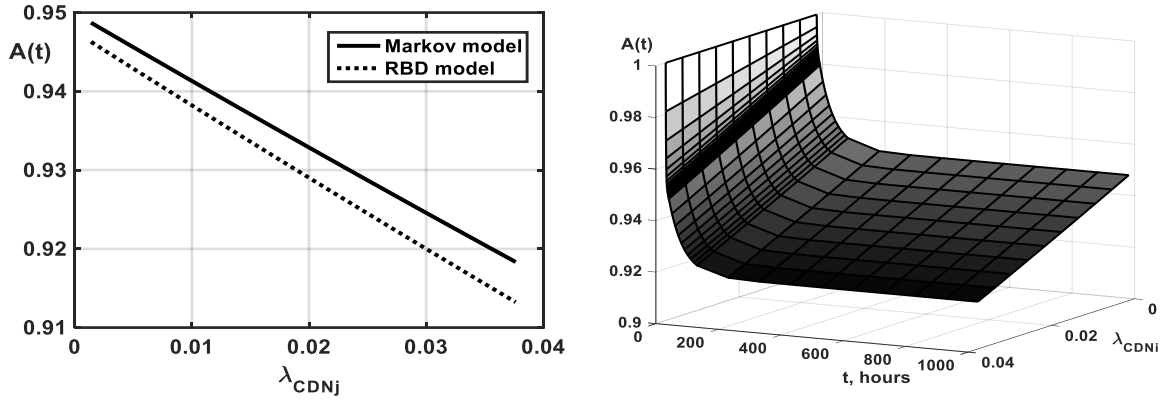
The simulation results showed that the difference between the cloud system availability indicators determined by RBD and Markov models have differences, not exceeding ΔA=0,0034. The weakest element in the architecture in the absence of attacks are end-user devices (DSM).

Figure 6,a illustrates the decrease in availability with increasing input parameter λ_{CDN}^{j} within the interval of Table.2. Estimates obtained using RBD and Markov models with increasing CDN failure rate increase the discrepancy from $\Delta A = 0.0034$ to $\Delta A = 0.0051$.

To solve systems of differential equations constructed according to the Kolmogorov-Chapman matrix, in the paper using the ode15s function [20]. The simulation results are shown in Figure 6,b. The change in time of the availability indicator, illustrated by the Markov model, shows the asymptotic direction of the function to a stationary value during the first t = 200 hours of CVS operation.

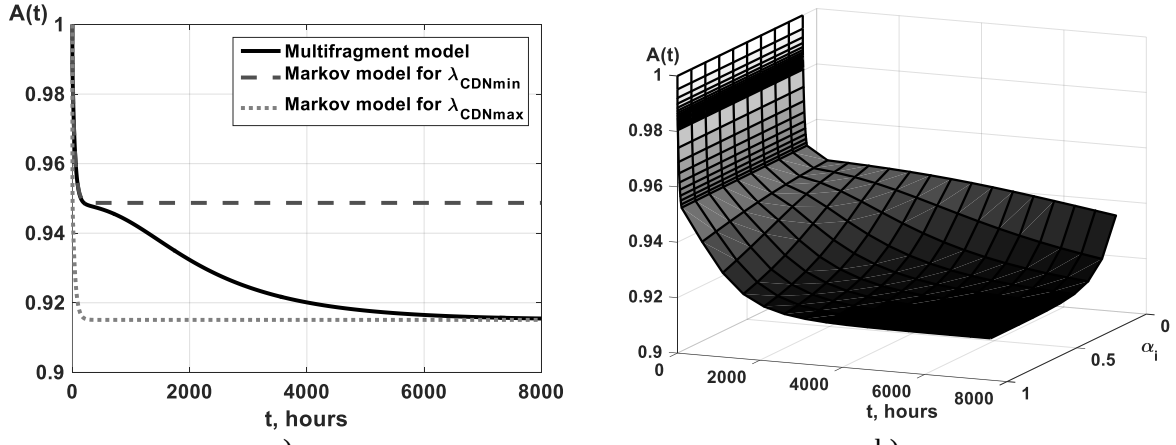
Table 3
Comparison of results of RBD and Markov models

# state	Element of system	Markov model Pi	RBD model Ai	Δ |Pi-(1-Ai)|
1	-	0,895362266	-	-
2	dsm	0,039793882	0,957446805	0,002759313
3	cdn	0,001243559	0,998613037	0,000143404
4	wifi	0,031977218	0,965517247	0,002505535
5	wifi / mnt	6,66E-04	0,99929627	3,75376E-05
6	mnt	0,018653381	0,979591837	0,001754783
7	aps1	0,001243559	0,998613038	0,000143404
8	qs	0,001165836	0,99869961	0,000134554
9	lb	1,07E-03	0,99881094	0,000123153
10	sgr	0,001492271	0,998336106	0,000171623
11	sgr/vpn	2,59E-06	0,999997116	2,9295E-07
12	vpn	0,001554448	0,998266898	0,000178654
13	aps2	0,003291773	0,996336997	0,000371231
14	aps3	0,002487118	0,997229917	0,000282966
A_{CVS}	CVS	0,949039584	0,945631343	0,003408241



a) b)

Figure 6: Results of RBD and Markov models (a) and Markov model (b) for different value λ_{CDN}



a) b)

Figure 7: Results of Markov and Multifragment models (a) and Multifragment model (b) for different value α

The results of availability modeling using a multifragment model are illustrated in Figure 7. Graphs in Figure 7,a allow you to compare the results of Markov and multifragment models. The availability function obtained by the MFM method reaches a stationary value after t = 8000 hours of operation, and the specified value of stationary availability is A = 0.9189. This indicator can be determined by a simpler Markov model, taking the value of the input parameter λ_{CDN} equal to λ_{CDN}^{max}.

Figure 7,b illustrates the influence of the input parameter α on the dynamics of changes in the availability function. The mechanism of influence of this parameter is as follows. As the parameter α increases, the time of transition of the availability function to stationary mode decreases, so for α = 0.5 t = 8000 hours; for α = 0.9 t = 4000 hours (that is twice as fast).

5 Conclusion

In the article, we presented the results of modeling to assess the availability of the cloud system. Two scenarios of events affecting system availability were considered: the first - in the absence of attacks on the CDN component; the second is in the case of attacks that cause an increase in the CDN failures rate to the limit level λ_{CDN}^{max}.

Parametrization of input data for the proposed models was performed using Machine Learning tools. In doing on, RDDs were formed from tuples of data that contained statistics on the reliability of CVS components. Next, the formed RDD datasets were transformed into matrix constructs, which were subjected to the operation of statistical testing of hypotheses (Hypothesis Testing) in accordance with the criterion of xi-square (Chi-square test).

A comparative analysis of RBD, Markov and Multifragment models was performed. The obtained results showed that the discrepancy between the stationary availability of RBD and Markov models is ΔA = 0.0034. As the CDN failure rate increases by an order of decimal order, this discrepancy increases to ΔA = 0.0051 (with the RBD model underestimating availability).

The conducted researches allowed to compare the results of Markov and multifragment models. The availability function obtained by the MFM method reaches a stationary value after t = 8000 hours of CVS operation, and the specified value of stationary availability is A = 0.9189. This indicator can be determined by a simpler Markov model, taking the value of the input parameter λ_{CDN} equal to λ_{CDN}^{max}. The influence of the input parameter α (probability of successful attack on the CDN component) on the dynamics of change of the availability function was also investigated with the help of a multifragment model. As the parameter α increases, the time of transition of the availability function to stationary mode decreases, so for α = 0.5 t = 8000 hours; for α = 0.9 t = 4000 hours (that is twice as fast).

Therefore, the choice of model strongly influences the assessment of the accuracy of the CVS stationary availability level and the time of transition of the availability function to the steady state. The presented results can be used by both developers and DevOps engineers to ensure effective functioning of the high available CVS. Future research directions can be connected with analysis of cloud multi-version architectures by use of DevOps tools.

6. References

[1] European Union Agency for Cybersecurity (ENISA). EUCS – CLOUD SERVICES SCHEME, 2020. URL: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[2] National Institute of Standards and Technology. NIST SP 500-291, Cloud Computing Standards Roadmap, 2013. URL: https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap.

[3] Lionel Sujay Vailshery, Distribution of cloud computing (IaaS, PaaS, SaaS) market revenues worldwide from 2015 to June 2021, by vendor. 2022, URL: https://www.statista.com/statistics/540511/worldwide-cloud-computing-revenue-share-by-vendor/

[4] K. S. Trivedi, A. Bobbio, Reliability and Availability Engineering. Modeling, Analysis and Applications, Cambridge, United Kingdom: Cambridge University Press, 2017. doi: 10.1017/9781316163047.

[5] T. Pinheiro, D. Oliveira, R. Matos, B. Silva, P. Pereira, C. Melo, P. Maciel, “The Mercury Environment: A Modeling Tool for Performance and Dependability Evaluation,” Ambient Intelligence and Smart Environments, vol. 29, pp. 16–25, 2021. doi: 10.3233/AISE210075
[6] G. Araújo, L. Rodrigues, K. Oliveira, I. Fé, R. Khan, and F. Silva, “Vehicular cloud computing networks: availability modelling and sensitivity analysis,” International Journal of Sensor Networks, vol. 36, no. 3, 2021, pp. 125–138. doi: 10.1504/IJSNET.2021.117229
[7] S. Distefano, and K. Trivedi, “Non-Markovian state-space models in dependability evaluation,” Quality and Reliability Engineering International, vol. 29, no. 2, 2013, pp. 225–239.
[8] D. Oliveira, J. Dantas, N. Rosa, P. Maciel, R. Matos, and A. Brinkmann, “A dependability and cost optimization method for private cloud infrastructures,” International Journal of Web and Grid Services, vol. 15, no. 4, 2019, pp. 367–393. doi:10.1504/IJWGS.2019.103222
[9] M. Di Mauro, G. Galatro, M. Longo, F. Postiglione and M. Tambasco, "Availability Analysis of IP Multimedia Subsystem in Cloud Environments," 2019 4th International Conference on System Reliability and Safety (ICSRS), 2019, pp. 111-115, doi: 10.1109/ICSRS48664.2019.8987674.
[10] J. Dantas, R. Matos, J. Araujo, and P. Maciel, “Models for dependability analysis of cloud computing architectures for eucalyptus platform,” International Transactions on Systems Science and Applications, vol. 8, no. 5, 2012, pp. 13-25.
[11] P. Zhang et al., "A Fault-Tolerant Model for Performance Optimization of a Fog Computing System," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1725-1736, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3088417.
[12] S.M. Farzaneh, O.Fatemi, "A novel virtual machine placement algorithm using RF element in cloud infrastructure." J Supercomput 78, 1288–1329, 2022. doi: 10.1007/s11227-021-03863-9
[13] O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak and K. Smoktii, "Semi-Markov's models for availability assessment of an Infrastructure as a Service Cloud with multiple pools of physical and virtual machines," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 98-102, doi: 10.1109/DESSERT.2018.8409107
[14] D. Maevsky, E. Maevskaya, A. Bojko and O. Besarab, "Transient in the Software Systems. Untraditional Approach to Software Reliability," 2019 International Conference on Information Technologies (InfoTech), 2019, pp. 1-4, doi: 10.1109/InfoTech.2019.8860879.
[15] R. Ushakov, E. Doynikova, E. Novikova and I. Kotenko, "CPE and CVE based Technique for Software Security Risk Assessment," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021, pp. 353-356, doi: 10.1109/IDAACS53288.2021.9660968.
[16] National vulnerability database (NVD), 2022.URL: https://nvd.nist.gov
[17] O. Ivanchenko, V. Kharchenko, B. Moroz, Y. Ponochovnyi and L. Degtyareva, "Availability Assessment of a Cloud Server System: Comparing Markov and Semi-Markov Models," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021, pp. 1-6, doi: 10.1109/IDAACS53288.2021.9661052.
[18] D. Novikov, "Systems Theory and Systems Analysis. Systems Engineering." In: Cybernetics. Studies in Systems, Decision and Control, vol 47. 2016. doi: 10.1007/978-3-319-27397-6_4
[19] Systems Engineering Body of Knowledge (SEBoK). SEBoK v. 2.5, 2021. URL: https://www.sebokwiki.org/w/images/sebokwiki-farm!w/2/24/SEBoKv2.5.pdf
[20] Solve stiff differential equations and DAEs – variable order method – MATLAB ode15s, 2022. URL: https://www.mathworks.com/help/matlab/ref/ode15s.html
[21] T. Duc, R. Leiva, P. Casari, P.-O. Östberg. "Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey." ACM Comput. Surv. 52, 5, 2020, pp. 1–39. doi: 10.1145/3341145
[22] S. Duvvuri, B. Singhal, Spark for Data Science. Packt Publishing Ltd. 2016.