


Article

Stochastic Approach to Investigate Protected Access to Information Resources in Combined E-Learning Environment

Radi Romansky 

Department of Informatics, Faculty of Applied Mathematics and Informatics, Technical University of Sofia, 1000 Sofia, Bulgaria; rrom@tu-sofia.bg

Abstract: The digital era expands the scope and application of information technologies, which also affects the forms of e-learning, motivating the development of combined systems with heterogeneous resources and services, including in the cloud. In this vein, the present article investigates the implementation of a set of procedures for maintaining regulated access to resources (identification, authentication, authorization, etc.) in a combined e-learning environment, with the main goal to confirm their effectiveness and correctness. The study was conducted through analytical modelling using stochastic tools from the theory of Petri nets and Markov chains with additional statistical analysis. The application of such a combined approach allows increased research efficiency and better adequacy of the obtained estimates.

Keywords: heterogeneous information resources; combined learning; data protection; security; regulated access

MSC: 37M21



Citation: Romansky, R. Stochastic Approach to Investigate Protected Access to Information Resources in Combined E-Learning Environment. *Mathematics* **2022**, *10*, 2909. <https://doi.org/10.3390/math10162909>

Academic Editors: Heui Seok Lim, Sanghyuk Lee, Yeongwook Yang and Imatitkua Aiyanyo

Received: 14 July 2022

Accepted: 9 August 2022

Published: 12 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The contemporary information society (ISoc) is increasingly associated with mass informatization [1], based on the growing role of new information technologies (IT) in the digital age. The computerization of various spheres of society has necessitated the increase of the efficiency of network communications [2] and the optimization of the management of information resources [3]. These aspects of informatization require the development of a strict framework of rules for access and use of resources allocated in the network space, including through mobile applications [4], which reflects on ensuring privacy and data protection in organizations [5]. It has been argued that a major feature of the modern digital age is the processing of knowledge and artificial intelligence, which raises the question of choosing an appropriate method [6]. This is also important in the development of e-learning, as the platforms are constantly expanding, both with intelligent systems [7] and with network solutions based on cloud computing [8].

The continuous development of e-learning systems is based on network communications and the services and environments offered, such as virtual reality, forums, social networks, chats, cloud, etc. This led to the realization of various forms of e-learning as a distributed learning (d-learning), mobile learning (m-learning), and different new models such as “cloud learning” [9], “collaborative learning” [10], “Micro-learning” [11], etc. All these innovative solutions of e-learning platforms require using adequate measures for information security and data protection. The socialization of network interactions also has an impact on the development of e-learning models because communication between people is directly related to human activity. They are inherent in the mental characteristics of people’s associations, having a direct impact on the personal space of each individual by stimulating social communication. Authors of [12] state that “socialization is a key mechanism of social reproduction” and reviews the specifics of historical aspects, alternative

concepts, and its use. A framework for a new theory of socialization based on cognitive science, pragmatism, language opportunities, and reassessment of values is proposed in this article.

The purpose of this article is to extend the case discussed in [13] to investigate the processes of protected access and secure use of resources in e-learning spaces with heterogeneous structure. The architecture proposed there is based on combining traditional e-learning tools with the capabilities of social communications and cloud computing. This heterogeneity of approaches and the applied means for multiple and distributed access require the application of procedures for regulating the access from different users (external and internal) to diverse information resources (educational materials, system files, profiles and personal data, journal service files, etc.). The investigation presented here is based on the Petri nets theory with their extension stochastic Petri nets (SPN) and using Markovian processes. The research is conducted on the basis of the author's procedure for organization of model investigation and presents a new extension to the applicability of the developed specialized program environment by using TryAPL2 to study processes at the macro-level. This determines the novelty of the proposal in this article which continues the investigation carried out in [13].

An overview of related works in the discussed field is presented in Section 2. Section 3 presents the object of research and the initial statement, and the main stochastic model investigation is discussed in Section 4.

2. Related Works

As stated in [1], the heterogeneous aspects of informatization set requirements for the development of an adequate policy for the functional capabilities of the network space. It is a technological, socio-economic, and cultural process with important changes in society, requiring the formation of an adequate information culture. Two main theoretical and methodological approaches to informatization are defined: technological approach (related to development of technical and technological means and tools oriented mainly to production and productivity) and sociological approach (considering informatization as an impact on all spheres of human activity with an impact on all individuals in society).

The first approach reflects on network communications and the conditions provided by corporate computer networks for information delivery and optimization of times for this. In [2], it is stated that due to the highly dynamic nature of the traffic, the current congestion of the communication channels has a significant impact on the delivery time. In this respect, development of mathematical and software support for multi-parameter routing is presented in this article. The goal is to help network protocols for constructing optimal delivery routes for delivering information to the receiver and efficient distribution of traffic flows over communication channels online. In addition, the sequence of actions for the formation of an optimization model and an algorithm for the intellectual support of the process of rating management of the distribution of resource support in the organizational system are discussed in [3]. An optimization model is proposed for the formation of extreme and borderline requirements in the formation of management tasks and decision-making based on a developed algorithm for intellectual support using a game approach to solving the block linear programming problem.

The second approach is directly related to the term "social", referring to the life of people in a certain society (social status), to the formation of separate social classes, and to communication between people (social contacts) [14]. In the structure of social communication, three mutually related sides can be distinguished: communicative side (communication in the narrow sense related to immediate exchange of information between communicating individuals); interactive side (organization of interaction between communicating individuals in the exchange of knowledge, ideas, and impacts); and perceptual side (characterizes the process of mutual perception of communication partners and establishment of mutual understanding).

The expanding possibilities of the digital society lead to the generation of massive information flows between communicating users in the network, which gives rise to the so-called “information avalanche”. Unfortunately, this abundance of information also has its unwanted effects [1]: devaluation of information; obtaining low-quality knowledge; spending too much time and attention on the part of users to “surf” the web; loss of productivity due to spam; additional costs related to data transfer, storage options, etc.; and security and privacy issues (not least). For this reason, it is necessary to discuss the problem with the user’s privacy and personal data protection in the network space. An important problem and the large volume of personal data for users stored in mobile devices, a method to protect this data by creating multiple safe virtual containers is proposed in [4]. The solution provides a data protection tool when developing mobile applications using special features of the Android operating system. A security analysis was also made with emphasis on the level of cryptographic strength of the proposed mechanism. On the other hand, the important problem with the user’s privacy and personal data protection in the digital age is discussed in [15], as the main recommendations of the latest European regulation GDPR (General Data Protection Regulation) to the presented and processed data in the network space are summarized in [5]. It is obvious that the growing informatization of society increases the risk of information security violations, as research in this direction related to cloud infrastructure and the principles of its management is presented in [16,17]. A similar risk also exists with technological solutions based on the Internet of Things (IoT), “smart” technologies for home, city, transport, etc. (cyber-physical systems—CPS), and accumulation of big data and their processing (Big Data analytics). A detailed study of users’ attitudes towards IoT, including their awareness of data privacy and security, was done in [18], where a model is proposed to formulate hypotheses about users’ trust in IoT processes. A summary of privacy issues in the contemporary smart society is given in [19], noting the need to transform management roles and activities to correspond to the modern digital technologies. The problem of personal privacy in digital space is well discussed in different articles and the conclusion is that increasing user demands for more services leads to the disclosure of more personal data, which increases the risk to privacy. The traditional solution to such problems is to strike a balance between the desired services and possible risks.

With the development of information technologies, the concepts of university education are also changing in order to meet the growing demands of market conditions. For example, in [7], a concept of an intelligent university based on the creation of intellectual resources is presented, the conditions for their management are specified, and an effective algorithm is proposed. In this direction, the discussion of the advantages of cloud technologies for increasing the possibilities of the educational process is also held in [8]. A technological solution for independent work with cloud resources is proposed, and the capabilities of the three main services (SaaS, IaaS, PaaS) are indicated. One important advantage of the article is the discussion of the issue of information security and possible problems when applying cloud technologies in education, defining 10 specific recommendations for “secure use of cloud technologies”.

The entry of the cloud into educational services is also discussed in [9], where a theoretical overview of the layers of cloud architectures and their relation to e-learning models is made. The conducted research allowed to define the main advantages of the application of cloud services in the educational strategy-convenient tools for e-education, effective organization of the learning process, preparation of content, effective tools for monitoring knowledge, etc. The article also discusses the issue for the organization of an effective information security and privacy system. In conclusion, it is stated that the study confirmed the usefulness of cloud computing for increasing the quality of educational content and e-learning processes. The idea of applying cloud technologies in e-learning environments is also defended in [10], where the possibility to “avoid the problem of overloading the institutions infrastructure resources, manage a large number of learners and improve collaboration and synchronous learning” is highlighted. An approach called

“Collaborative Learning Process in Cloud” is proposed, including two steps—designing a common process for hiring cloud services and developing a functional algorithm and awareness discovery module. An addition to the discussed problems is the article [11], which points to micro-learning as a suitable solution for e-learning. The concept is based on “breaking” the learning content into small fragments for easier absorption by the learners and use in short periods of time. To this end, an updated overview of this learning paradigm is provided and the application of micro-learning in more formal distance learning environments is discussed.

Investigating processes in the network space is a fairly common approach, both before design and when improvements are needed. In many cases, this is also related to the growing volume of data collected, which leads to privacy risks. One applied research possibility is the theory of Petri nets (PN), using the different versions—classical, temporal (TPN), stochastic (SPN), coloured (CPN), etc. The stochastic approach based on SPN and Markov processes is widely used in various areas of the digital world. This approach is used in [20] to determine the failure rate of software components of a modular system and in [21] to evaluate the performance of complex industrial systems. In both cases, research shows better results than applying other methods. The applicability of the SPN-apparatus is also confirmed by an article [22] in which the possibility of adjusting the queues in a health department in case of changing staff absence is investigated. The goal is to make a proper resource planning, using the Petri net combined with mathematical formalization, simulation, and graphical interpretation of the results. The stochastic approach has also been used by other researchers, for example a system for predicting failures for certain periods of time is proposed in [23] with investigation of the two regimes (transient and stationary) of probabilistic processes. In addition, a model for analyzing and verification by applying the matrix-analytical method is developed. This has allowed their correct application in the respective field for which they were developed.

A widely used stochastic approach in the scientific space is based on Markov models and, in particular, on Markov chains. In this direction is the investigation presented in [24] of functional safety in evaluating the safe operation of a real CPS for calculation of the metric criteria in expert evaluation of the system. A spatial model was created as a Markov chain and a statistical analysis of the results was carried out. Advantages such as reduction of empirical data, compactness of the obtained data, simplicity of interpretation of the results, etc. are indicated. The apparatus of Markov chains was also used in [25] in estimating the number of samples for the purpose of optimization, being supplemented with the Monte Carlo method to obtain robust Bayesian analysis and conclusions. Another view of Markov models is presented in [26], where a Hidden Markov Model with a quasi-power relation kernel based on prognostic information was developed to study the influence of service age on its performance. It is indicated that the developed improved genetic algorithm can successfully replace the conventional one for parameter estimation, and the study confirms the better effectiveness.

3. Initial Definition of the Research Problem

Cloud computing is a technology for dedicated data processing through virtual machines in the global network, which allows increasing data processing and storage capacities without a significant increase in investment. The model allows for cost savings and increased IT flexibility, but use must be based on a serious prior risk analysis for data, including personal data. The latter requires addressing known interoperability, security, and data portability issues.

Another specific feature of the network space is the provision of various tools and opportunities for social communication and resource sharing. This creates the conditions for building the so-called “collective intelligence”, which is a set of Internet users who gather and share content to create something new that is impossible for man himself. This is realized on the basis of the Social Web—a community of interconnected people who interact through conversations or participation with content through the global network.

In general, the result is “social computing” representing a joint interactive aspect of online behavior, created as a result of the development of Internet communications and the ability to exchange different types of information. This concept unites activities in the global network in which users are not only passive participants, but also implement various forms of direct communication, information sharing, and opening their own profiles. Globally, the term should be seen as a complex of different web-based and mobile technologies that allow transforming traditional communication into interactive dialogue by sharing photos, images, audio, video, experience, and other resources, as well as creating, editing, and distribution of content on the Internet.

The analysis allows defining an initial concept for a combined space of resources used to provide education services, presented in Figure 1. The main communication environment is the global network, but there is possibility for direct access, mainly to internal resources, which in addition to educational information contain profiles with personal data of employees, teachers, and registered participants, as well as system files to maintain regulated access to the whole information environment.

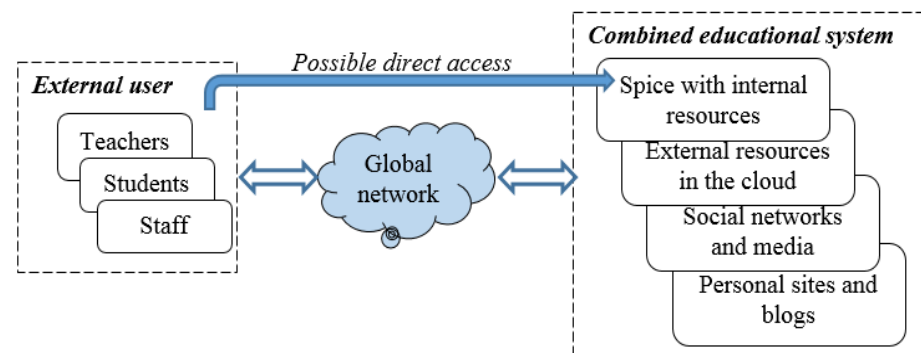


Figure 1. Conceptual model for a combined e-learning environment.

In the proposed conceptual model, the main information resources of the learning environment are located both in internal memory spaces and in cloud data centers. The use of a virtual cloud environment requires a serious risk analysis, because at least three main concerns regarding the privacy of customers when using cloud services can be defined:

- ✓ Possible vulnerability to attacks because, in principle, critical business information and resources are outside the customer’s secure environment.
- ✓ Standard security practices are most often used, which in most cases require disclosure and inspection, and this raises legitimate concerns for the customer about the privacy of user data.
- ✓ There are not always categorical declarations by cloud providers to comply with European Union privacy regulations, which do not allow the transfer of certain categories of personal data. Data in the cloud are stored in various locations around the world, and this may lead to violations of these regulations.

The new EU regulation (GDPR) introduced fundamental requirements to the digital space and in particular to digital (and cloud) service providers, such as:

- ✓ Requirement to give explicit and fully informed consent to the collection and use of personal data.
- ✓ Users get the opportunity to control their personal data.
- ✓ Easier access to own personal data.
- ✓ Network service providers are obliged to inform users in a clear, comprehensible and transparent way about how the provided data will be used.
- ✓ Provision of rights to portability of personal data when they are transferred from one provider to another.

Various possible risks to cloud data security can be defined, some of which are summarized in Table 1.

Table 1. Possible risks for data security in the cloud.

<i>Basic Requirements</i>	<i>Comment for the Possible Risk</i>
Confidentiality of information	The access of many users to information stored in the cloud is a risk to its confidentiality and this requires reliable information security based on the “CIA” triad, ensuring access only to authorized persons.
Sharing link	This approach is convenient for sharing data with various business partners but creates the conditions for a breach in system security and data leakage to an unauthorized domain.
Multi-tenancy	There is a possible risk of violating the integrity and availability of supported data, as well as the possibility of unauthorized access causing deletion, modification, theft.
Residual data	Possibility for non-full deleting or removing all copies of data in the cloud create the risk to violate of the main requirement “right to be forgotten/erased”.
Privacy of the software	It must ensure that each application or process in the cloud maintains and processes the information in a secure and reliable manner.
Integrity and availability	Multiple access to cloud resources creates a risk for the supported data and this requires their protection by means of unauthorized access and breach of data integrity by deletion, modification, theft, etc.
Integration of production directories	In business, this is done for single-sign-on (SSO) purposes, with most direct communication systems integrating authentication with existing production systems, but this creates a risk to the supported information when accessing it.

4. Structural Organization of a Combined E-Learning Environment

The defined possible risks for the processes in the combined e-learning space require the introduction of strict procedures to check the legitimacy of access and the specific rights to use a certain type of resources. This should be reflected even at the level of architectural design, as a generalized architectural model is proposed in [13]. Two interconnected, but relatively independent sub-systems are distinguished, between which the main procedures are distributed (Figure 2).

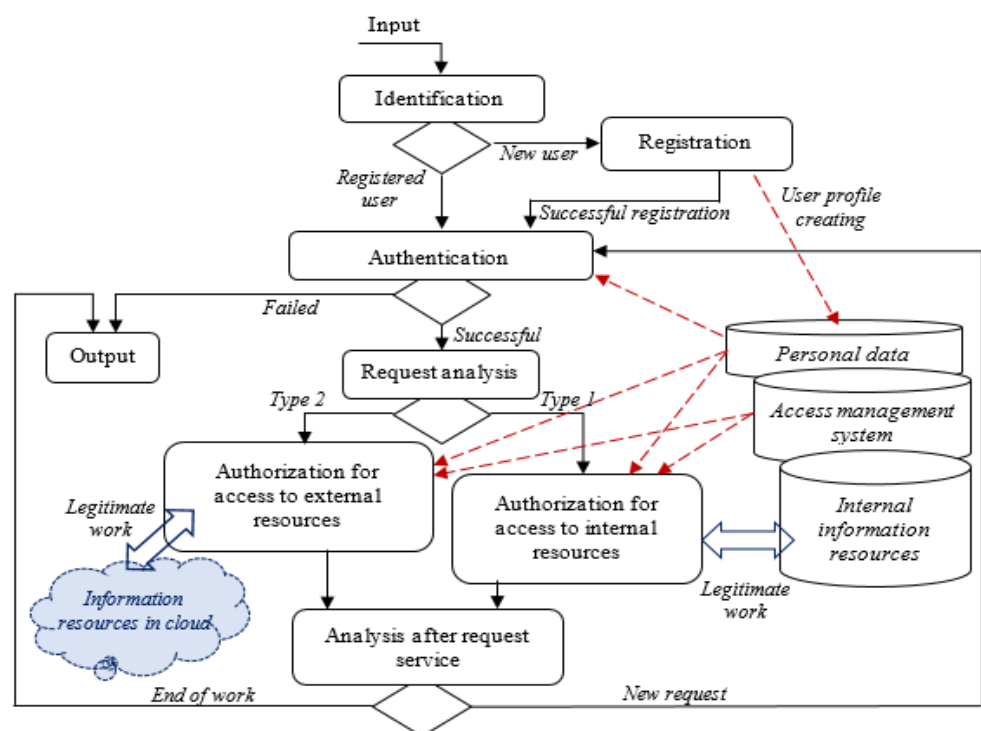


Figure 2. Formalization of processes for access regulation.

- ✓ Front Office (Communication System) for supporting all communications with users during remote access to resources and their preliminary identification based on registration. The role of this system is to support initial information security procedures, such as registration, identification, and preliminary authentication of user’s request. An important task of this “input point” is to create and maintain system data files for legitimate users or log files for unregistered access attempts.
- ✓ Back Office (Management System) to ensure high reliability of processes when servicing approved user requests based on resource protection and data security requirements. This internal system conducts the administration after evaluating the legitimacy of the requests and the level of granted access rights to the requested resources, maintaining specialized procedures for the analysis of requests, type of access and its authentication, as well as a strict authorization. The functionality of the components of this system is distributed among three basic sub-systems—administrative, information, and experimental, each of them with defined access to certain databases supporting the respective resources.

5. Model Investigation of the Functionality

5.1. Short Presentation of the Initial PN-Model

Different approaches are known for organizing a model study of a given object at the stage of its preliminary development. In general, they can be divided into deterministic and stochastic, each with its own advantages and disadvantages and with a variety of platforms and programming environments for experiment automation. The research presented below is based on a defined initial model of the investigated object as a Petri net (PN) with an analytical description $PN = \{T, P, I, O\}$, for $T \cap P = \emptyset$ with the theoretical-set definition presented in Figure 3.

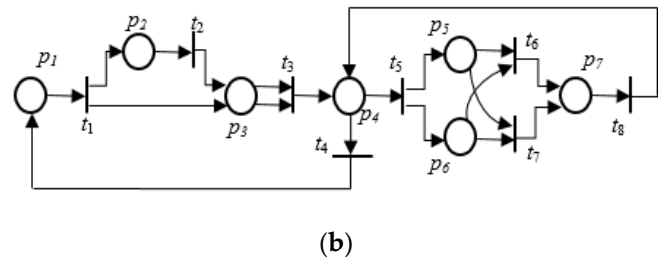
Input functions:

- $I(t_1) = \{p_1\}$
- $I(t_2) = \{p_2\}$
- $I(t_3) = \{p_3, p_3\}$
- $I(t_4) = \{p_4\}$
- $I(t_5) = \{p_4\}$
- $I(t_6) = I(t_7) = \{p_5, p_6\}$
- $I(t_8) = \{p_7\}$

Output functions:

- $O(t_1) = \{p_2, p_3\}$
- $O(t_2) = \{p_3\}$
- $O(t_3) = \{p_4\}$
- $O(t_4) = \{p_1\}$
- $O(t_5) = \{p_5, p_6\}$
- $O(t_6) = O(t_7) = \{p_7\}$
- $O(t_8) = \{p_4\}$

(a)



(b)

Figure 3. Definition of the proposed PN-model. (a) Analytical definition; (b) graph presentation of the PN-model.

Transitions (procedures): t_1/t_2 —identification of incoming request (registered/unregistered); t_3 —authentication procedure; t_4 —exit from the system; t_5 —analysis of a legitimate request for access; t_6/t_7 —two types of authorization procedure in reason request for access to external / internal resources; t_8 —end of the current service.

Positions (conditions): p_1 —presence of a request for access; p_2/p_3 —request from unregistered/registered user); p_4 —result after authentication (legitimate or illegitimate access); p_5/p_6 —request with certain access to external/internal resource; p_7 —request for next action.

The execution of the PN-model is illustrated by the tree of reachability shown in Figure 4 with an initial situation marked by $\mu_0 = (1,0,0,0,0,0,0)$ allowing the activation of transition t_1 . The presented evolution of the analytical model is based on the permitted transitions.

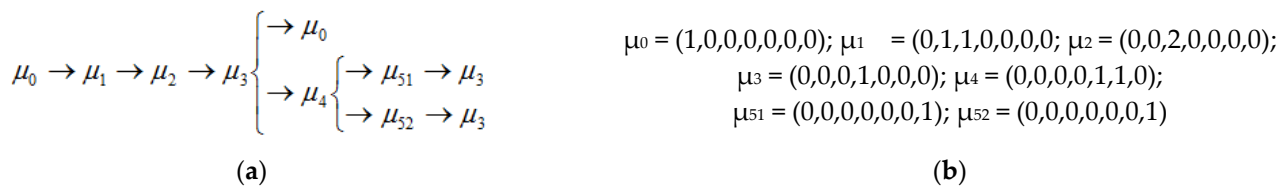


Figure 4. Evolution of the analytical PN-model. (a) Tree of reachability; (b) active markings.

5.2. Stochastic Extention of the Model Investigation

5.2.1. Preliminary Discussion

The research presented in this section is an extension of the above to confirm the obtained analytical results for the evolution of the model by applying a stochastic approach. The classical version of PN allows to define a discrete structure of the deterministic model of the investigated object. It can be extendable by using the Timed Petr Net apparatus, which permits to describe the system under study by an ordered structure TPN: = (P,T,I,O,Θ) with the additional set Θ = {θ₁, θ₂, . . . , θ_n} of elements to describe possible delays θ_i = θ(t_i) when executing the defined transitions.

In the case considered here, an opportunity to reflect the probabilistic nature of the processes is sought, applying the Stochastic Petri Net (SPN) apparatus. It is based on the general formal definition SPN: = (P,T,I,O,L), which is ordered structure extending the classical PN-definition with the set L = {λ₁, . . . , λ_n}, the element of which represent the intensities of the transitions λ_i = 1/θ_i.

The SPN apparatus is based on Markovian processes with discrete states S = {s₁, . . . , s_n}, which correspond to the marks (s_i ≡ μ_i) determined during the execution of the network with probabilistic transitions between them. This makes it possible to define a stochastic analytical model as a Markov chain and to investigate the entry (falling) of the process into a stationary regime.

5.2.2. Definition of SPN

- ✓ Set of states |S| = 7 with elements reflecting the markings from the reachability tree of Figure 4 with the following compliance: S = {s₀ ↔ μ₀, s₁ ↔ μ₁, s₂ ↔ μ₂, s₃ ↔ μ₃, s₄ ↔ μ₄, s₅ ↔ μ₅₁, s₆ ↔ μ₅₂}
- ✓ Vector of initial probabilities: P₀ = {1, 0, 0, 0, 0, 0, 0}, determined based on the initial marking μ₀ for starting the model execution.
- ✓ Matrix of transition probabilities (Figure 5) reflecting transitions between successive markings, respectively between hierarchical levels in the reachability tree.

	s ₀	s ₁	s ₂	s ₃	s ₄	s ₅	s ₆
s ₀	0	1	0	0	0	0	0
s ₁	0	0	1	0	0	0	0
s ₂	0	0	0	1	0	0	0
s ₃	a	0	0	0	1-a	0	0
s ₄	0	0	0	0	0	b	1-b
s ₅	0	0	0	1	0	0	0
s ₆	0	0	0	1	0	0	0

Figure 5. Matrix of transition probabilities.

5.2.3. Analytical Formulation of the Model

The matrix of transition probabilities allows to draw up a directed graph of the states showing the development of the reachability tree during the execution of the processes in the studied system—Figure 6a. The established transitions between the markings (the states

of the Markov chain) define the relationships and dependencies between the individual probabilities and create the stochastic model—Figure 6b.

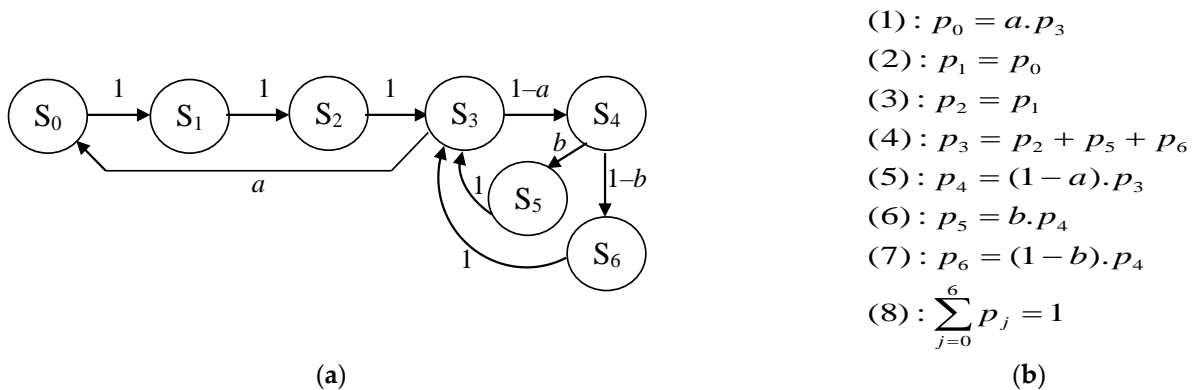


Figure 6. Definition of the model as a SPN. (a) Graph of the states of the Markov chain(graph definition); (b) stochastic analytical model.

5.2.4. Analytical Solution of the Stochastic Model

$$\begin{aligned}
 p_1 &= p_2 = p_0 \\
 p_0 &= a \cdot p_3 \Rightarrow p_3 = \frac{1}{a} \cdot p_0 \\
 p_4 &= (1 - a) \cdot p_3 = (1 - a) \cdot \left(\frac{1}{a} \cdot p_0\right) = \frac{1-a}{a} \cdot p_0 \\
 p_5 &= b \cdot \left(\frac{1-a}{a} \cdot p_0\right) = \frac{b \cdot (1-a)}{a} \cdot p_0 \\
 p_6 &= (1 - b) \cdot \left(\frac{1-a}{a} \cdot p_0\right) = \frac{(1-a) \cdot (1-b)}{a} \cdot p_0
 \end{aligned}$$

$$\sum_{j=0}^6 p_j = 1 \Rightarrow 3 \cdot p_0 + \frac{1}{a} \cdot p_0 + \frac{1-a}{a} \cdot p_0 + \frac{b-ab}{a} \cdot p_0 + \frac{1-a-b+ab}{a} \cdot p_0 = 1$$

$$p_0 \left(3 + \frac{1}{a} + \frac{1-a}{a} + \frac{b-ab}{a} + \frac{1-a-b+ab}{a} \right) = 1$$

$$p_0 \cdot \frac{1}{a} \cdot (3a + 1 + 1 - a + b - ab + 1 - b - a + ab) = 1 \Rightarrow p_0 = \frac{a}{a+3} = p_1 = p_2$$

$$p_4 = \frac{1-a}{a} \cdot p_0 = \frac{1-a}{a} \cdot \frac{a}{a+3} = \frac{1-a}{a+3}$$

$$p_5 = \frac{b \cdot (1-a)}{a} \cdot \frac{a}{a+3} = \frac{b \cdot (1-a)}{a+3}; p_6 = \frac{(1-b) \cdot (1-a)}{a} \cdot \frac{a}{a+3} = \frac{(1-b) \cdot (1-a)}{a+3}$$

As a result of the analytical solution of the model, the following expressions for the final probabilities in steady state are obtained:

$$p_0 = p_1 = p_2 = \frac{a}{a+3} \dots; p_4 = \frac{1-a}{a+3} \dots; p_5 = \frac{b \cdot (1-a)}{a+3}; p_6 = \frac{(1-b) \cdot (1-a)}{a+3}$$

5.2.5. Statistical Estimations and Graphical Presentation

To conduct the investigation, a set of values for the controllable parameters *a* and *b* is defined. The selection of specific values was made by taking into account their compliance with the expected average statistical estimate for the realization of the transitions between the states (from *S*₃ and *S*₄ to the others). On this basis, the finite set of values {0,1; 0.2; 0.3; 0.4; 0.5; 0.6; 0.7; 0.8; 0.9; 1} is determined for the parameter *a*, and for parameter *b* a variation

range of 0.3 to 0.7 is specified with a variation step $\Delta = 0.1$. Under these initial conditions, a complete factorial plan is realized for the selected levels of the controllable parameters a and b . Figure 7 presents a graphical interpretation of the generalized experimental results for the mean-statistical estimates of the final probabilities in the steady state.

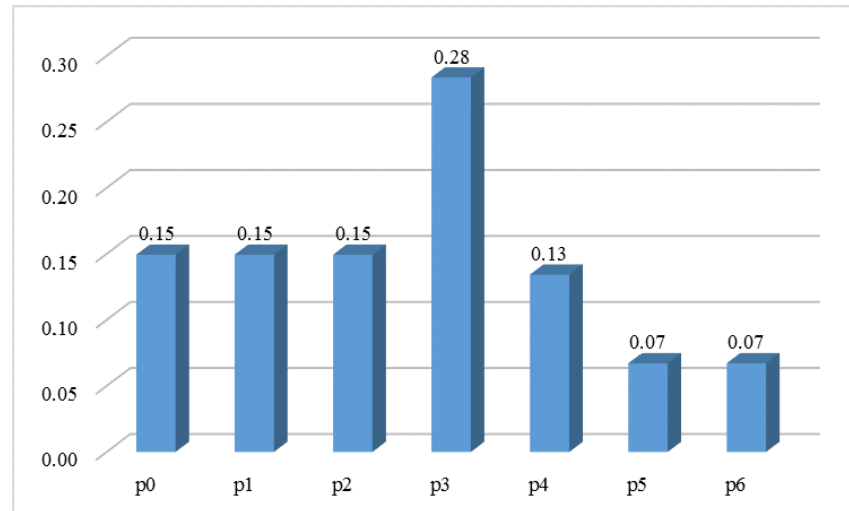


Figure 7. Average estimates for the final probabilities in the implementation of a complete factor plan with values $a = 0.1 \div 1.0$ ($\Delta = 0.1$) И $b = 0.3 \div 0.7$ ($\Delta = 0.1$).

Figure 8 presents a summary of experimental data at a fixed mean value for parameter b and varying the other controllable parameter a . These two controllable factors are directly related to the transitions when checking the authorization of access to an external or internal resource (transitions t_6 and t_7 in the PN model and, respectively, transitions from state S_4 to S_5 and S_6 of the Markov chain). The case of uniform distribution of requests between two resources is investigated, while parameter a , related to determining the level of legitimacy of requests and/or stopping work with the system, is assumed to vary in the range from 0.2 to 0.9 with step $\Delta = 0.1$.

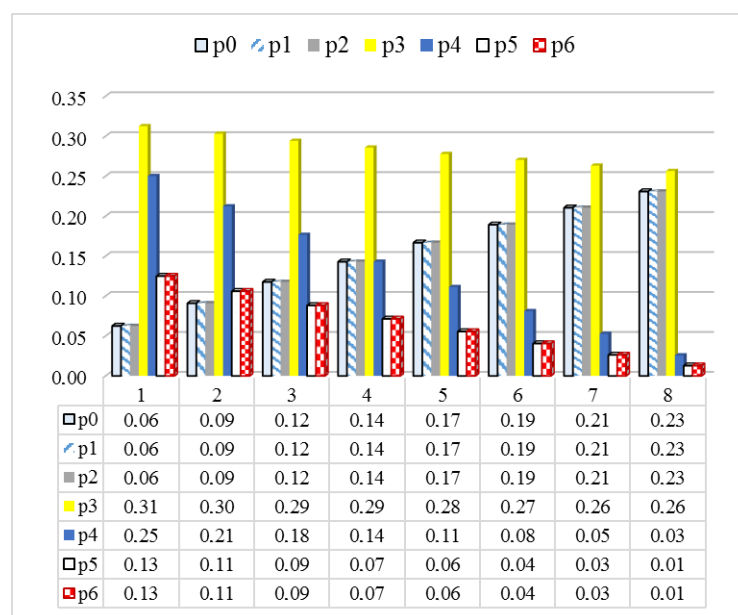


Figure 8. Statistical sample of the final probabilities for the controllable parameters $b = 0.5$ and $a = \{1 = 0.2; 2 = 0.3; 3 = 0.4; 4 = 0.5; 5 = 0.6; 6 = 0.7; 7 = 0.8; 8 = 0.9\}$.

Estimates show that the highest values for all situations are for probability p_3 corresponding to state S_3 . This state is associated with transitions t_4 and t_5 , which support the procedures for authentication and authorization of the information security system. The equality of the estimates for the probabilities p_5 and p_6 is justified because of the average value of the parameter b . There is a direct dependence of the tendency to decrease the relative occupancy of the permit procedure (probability p_4) with an increase in the price of the parameter a .

6. Conclusions

The main goal of the article is to present selected results of a study of the processes of managing access to information resources in a distributed learning environment with a combined composition, including cloud services. In practice, this is one stage in the overall development and research of the heterogeneous environment, and here a stochastic approach is applied to further confirm the reality of the results obtained from previous studies. In this case, to further analyze the results of a model study through a classical Petri net, a model based on the stochastic variant SPN was developed, reflecting the probabilistic nature of the processes in the digital space. This is appropriate and necessary because it is known that the network space as a whole is characterized by a discrete structure, but the processes of service provision, their request by different users, and their use have a probabilistic nature, especially with multiple access and competition of user requests. The latter, as discussed above, creates a privacy risk as well as opportunities to violate the CIA triad (Confidentiality, Integrity, Availability) requirements.

The main contribution is the analytical formulation of the SPN-model and its solution to determine the analytical expressions for the individual probabilities of falling into the hierarchical levels of the reachability tree, reflecting the evolution of the model and from there, the development of the processes in a studied system. In addition, a statistical analysis was performed, evaluations were presented for the execution of selected factorial plans, and their graphical interpretations were also shown.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Romansky, R. Informatization of the society in the digital age. *Biomed. J. Sci. Tech. Res.* **2021**, *33*, 25902–25910. [[CrossRef](#)]
2. Kravets, O.J.; Atlasov, I.V.; Aksenov, I.A.; Molchan, A.S.; Frantsisko, O.Y.; Rahman, P.A. Rahman. Increasing efficiency of routing in transient modes of computer network operation. *Int. J. Inf. Technol. Secur.* **2021**, *13*, 3–14.
3. Cheryshov, A.B.; Choporov, O.N.; Preobrazhenskiy, A.P.; Kravets, O.J. The development of optimization model and algorithm for support of resources management in organizational system. *Int. J. Inf. Technol. Secur.* **2020**, *12*, 25–36.
4. Glet, M.; Kaczyński, K. Secret sharing scheme for creating multiple secure storage dimensions for mobile applications. *Int. J. Inf. Technol. Secur.* **2020**, *12*, 83–102.
5. Tzolov, T. Data model in the context of General Data Protection Regulation. *Int. J. Inf. Technol. Secur.* **2017**, *9*, 113–122.
6. Kasabov, N. From multilayer perceptrons and neurofuzzy systems to deep learning machines: Which method to use?—A survey. *Int. J. Inf. Technol. Secur.* **2017**, *9*, 3–24.
7. Berdnikova, L.F.; Mikhaleuk, N.O.; Pavlova, S.V.; Gortcevskaia, O.G.; Krivtsov, A.I. Intellectual resources in the development of smart university. In *Smart Education and E-Learning*; Part of “Smart Innovation, Systems and Technologies”; Springer: Singapore, 2020; Volume 188.
8. Zaslavskaya, O.Y.; Zaslavskiy, A.A.; Bolnokin, V.E.; Kravets, O.J. Features of ensuring information security when using cloud technologies in educational institutions. *Int. J. Inf. Technol. Secur.* **2018**, *10*, 93–102.
9. Wu, W.; Plakhtii, A. E-learning based on cloud computing. *Int. J. Emerg. Technol. Learn.* **2021**, *16*, 4–17. [[CrossRef](#)]
10. Sameh, A.; Hajlaoui, J.; Zaki, B.; Sonia, A.G. Collaborative e-learning process discovery in multi-tenant cloud. *Int. J. Intell. Syst. Appl.* **2021**, *13*, 21–37.
11. Díaz Redondo, R.P.; Caeiro Rodríguez, M.; López Escobar, J.J.; Fernández Vilas, A. Integrating micro-learning content in traditional e-learning platforms. *Multimed. Tools Appl.* **2021**, *80*, 3121–3151. [[CrossRef](#)]

12. Guhin, J.; McCrory Calarco, J.; Miller-Idriss, C. Whatever happened to socialization. *Annu. Rev. Sociol.* **2021**, *47*, 109–129. [[CrossRef](#)]
13. Romansky, R.; Noninska, I. Deterministic model investigation of processes in a heterogeneous e-learning environment. *Int. J. Hum. Cap. Inf. Technol. Prof.* **2022**, *13*, 1–16. [[CrossRef](#)]
14. Kolishev, N. Theory and Practice of Social Communications. Available online: <http://drugi.dokumentite.com/art/teoriq-i-praktika-na-socialnite-komunikacii/82661> (accessed on 12 July 2022). (In Bulgarian).
15. Romansky, R. Privacy and data protection in the contemporary digital age. *Int. J. Inf. Technol. Secur.* **2021**, *13*, 99–110.
16. Tsaregorodtsev, A.V.; Kravets, O.J.; Choporov, O.N.; Zelenina, A.N. Information security risk estimation for cloud infrastructure. *Int. J. Inf. Technol. Secur.* **2018**, *10*, 67–76.
17. Tsaregorodtsev, A.V.; Lvovich, I.Y.; Shikhaliev, M.S.; Zelenina, A.N.; Choporov, O.N. Information security management for cloud infrastructure. *Int. J. Inf. Technol. Secur.* **2019**, *11*, 91–100.
18. Koohang, A.; Sargent, C.S.; Nord, J.H.; Paliszkievicz, J. Internet of Things (IoT): From awareness to continued use. *Int. J. Inf. Manag.* **2022**, *62*, 102442. [[CrossRef](#)]
19. Kim, S.; Andersen, K.N.; Lee, J. Platform government in the era of smart technology. *Public Adm. Rev.* **2022**, *82*, 362–368. [[CrossRef](#)]
20. Zhijun, W.; Haolin, M.; Meng, Y. Reliability assessment model of IMA partition software using stochastic Petri nets. *IEEE Access* **2021**, *9*, 25219–25232. [[CrossRef](#)]
21. Kumar, A.; Kumar, V.; Modgil, V.; Kumar, A. Stochastic Petri nets modelling for performance assessment of a manufacturing unit. *Mater. Today Proc.* **2022**, *56*, 215–219. [[CrossRef](#)]
22. Kang, C.W.; Imran, M.; Omair, M.; Ahmed, W.; Ullah, M.; Sarkar, B. Stochastic-Petri Net modelling and optimization for outdoor patients in building sustainable healthcare system considering staff absenteeism. *Mathematics* **2019**, *7*, 499. [[CrossRef](#)]
23. Montoro-Cazorla, D.; Pérez-Ocón, R. Optimizing costs in a reliability system under Markovian arrival of failures and reposition by *K*-policy inspection. *Mathematics* **2022**, *10*, 1918.
24. Kovtun, V.; Izonin, I.; Gregus, M. The functional safety assessment of cyber-physical system operation process described by Markov chain. *Sci. Rep.* **2022**, *12*, 7089. [[CrossRef](#)] [[PubMed](#)]
25. Cruz, I.R.; Lindström, J.; Troffaes, M.; Sahlin, U. Iterative importance sampling with Markov chain Monte Carlo sampling in robust Bayesian analysis. *Comput. Stat. Data Anal.* **2022**, *176*, 107558. [[CrossRef](#)]
26. Liu, Q.; Chen, X.; Dong, M.; Chen, F.F. A novel health prognosis method for system based on improved degenerated Hidden Markov model. *Robot. Comput.-Integr. Manuf.* **2022**, *78*, 102402. [[CrossRef](#)]