axioms

MDPI

Article

Mathematical Model Investigation of a Technological Structure for Personal Data Protection

Radi Romansky [1,*]

[1,] Ttechnical University of Sofia, Bulgaria; rrom@tu-sofia.bg
* Correspondence: rrom@tu-sofia.bg

Abstract: The contemporary digital age is characterized by massive using different information technologies and services in the cloud. This sets the question "Are personal data processed correct in the global environments". It is known, that there are many requirements which Data Controller must perform. In this reason, the article presents a point of view for transfer some activities for personal data processing from traditional system to cloud environment. The main goal is to investigate what is difference between the two versions of data processing. For this goal a preliminary deterministic formalization of the two cases by using Data Flow Diagram is made. The second phase is organization a mathematical (stochastic) model investigation on the base of Markov chain apparatus. Analytical models are designed and their solution is made. Discussion of obtained assessment based on graphical presentation of analytical results is presented.

Keywords: personal data protection; cloud; formalization; data flow diagram; Markov chain; stochastic investigation; analytical assessments.

MSC: 37M21

1. Introduction

The contemporary Information Society (InSoc) is characterized by massive informatization and penetration of digital technologies in all areas, determined in [1] as "*the most recent long wave of humanity's socioeconomic evolution*" with the emphasis that the current digital age "*focuses on algorithms that automate the conversion of data into actionable knowledge*". The massive globalization of processes leads to increased activity in the Internet space with a reflection on the efficiency of the data network [2] due to increased access to remote resources and use of cloud data centres [3], data sharing in virtual environments [4], Internet of Things (IoT), including sensor collection of personal data [5] and others. For example, the last cited article confirms that today's advanced sensor technologies "*generate a large amount of valuable data*" for different applications as "*health care, elderly protection, human activity abnormal detection, and surveillance*". A result of technologies in the digital space is the dissemination of personal data (freely or unknowingly), which raises the serious question of the privacy of users and the reliable protection of their personal data. This requires that when developing environments for remote multiple access, organizational and technical measures to protect the data provided to users are foreseen. A basic requirement should be countermeasures against illegal distribution of user data and their use for purposes other than those announced, including the introduction of strict rules for authorization and authentication [6]. One direction of regulating the access and use of objects and data is discussed in [7], where it is emphasized that building systems with multiple services increases the security impact compared to the monolithic style. In order to answer important security questions in complex environments, a systematic review of

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Received: date
Accepted: date
Published: date

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

the main challenges in using the mechanisms and technologies for authentication and authorization in micro services is done.

The purpose of the article is to present a point of view of the technological organization of personal data protection processes in an example environment (administrative system) that uses cloud services and data centres and applies the requirements of the CIA triad (Confidentiality, Integrity, Availability). The requirements of this triad and their implementation in various technological solutions are well discussed. For example, a holistic study of the shortcomings of existing technological solutions for IoT and cyber physical systems (CPS) is presented in [8] and a solution through blockchain technology is proposed with an analysis of similarities and differences. Another research directed "*on the improvement of CIA triad to reduce the risk on online banking system*" is presented in [9].

Cloud computing allows taking advantage of the leasing of infrastructure, software and platforms offered as cloud services (IaaS, SaaS, PaaS). In this way, the costs of maintaining and administering own assets are reduced, and for the user, the "cloud" is a virtual environment for data processing and storage. The services offered provide various cloud capabilities, requiring proper pre-allocation of resources to overcome congestion, resource loss, load balancing, Quality of Service (QoS) violation, migration of virtual machines (VM), etc. A primary goal in the cloud is to correctly map VM to physical machines (PM) so that the PM can be effectively used. In this respect, an extensive survey of cloud resource management schemes is presented in [10] in order to identify the main challenges and point out possible future research. Another research conducted in [11] discusses cloud service reliability that should be further evaluated in specific conditions, and the paper proposes an approach based on combining cloud service reliability indicators to obtain effective evaluation and improve data security. Despite cloud service providers' claims of good information security at the platform level, doubts are being expressed about the protection of personal data. To overcome possible problems, a patent has been registered to define a "Data Protection as a Service" (DPaaS) paradigm for generating dynamic updates of the data protection policy using the machine learning model and comparison with previous instructions [12].

One of the applied approaches in researching processes in various systems and applications is modelling based on an appropriate apparatus and instrumentation. For example, simulation modelling has been applied in [13] to study the probabilistic behaviour and timing characteristics of interdependent tasks of arbitrary duration. The goal is to estimate the duration of the project and the possible risks of untimely completion. Another approach is the development of a mathematical description of processes, as was done in [14] to study the possibilities of minimizing power losses in a distribution transformer and evaluating energy efficiency. The proposed mathematical model describes the relationship between all parameters of the transformer by using the direct global iterative algorithm technique.

It is known that processes developing in systems most often have a probabilistic nature, which determines the effectiveness of the stochastic approach to research, and Markov processes and, in particular, Markov chains (MC) are a suitable apparatus. An example of this is the application of MC to study technological limitations in stochastic normalizing flows presented in [15]. Another application of MC is discussed in [16], where it is combined with the Monte Carlo method for assessing the characteristics of probability distributions and a review of "*methods for assessing the reliability of the simulation effort, with an emphasis on those most useful in practically relevant settings*" is made. In addition, the strengths and weaknesses of these methods are discussed.

The main goal is to carry out a preliminary study of the constructed structural objects of the designed administrative system and the processes supported by them, applying the apparatus of Markov chains (MC). The choice of the tool is determined by the stochastic nature of the processes in an essentially discrete hardware (computer) environment. To conduct the experiments, an author's programming environment, developed in the APL2 language [17], was used, and a graphic interpretation of the evaluations was additionally

made. An approach using MC to conduct model research is applied in [11] to study the reliability of network services as well as in [18] to investigate basic performance and optimization measures in resource planning in the cloud and in IoT with in order to improve performance and QoS. An efficient algorithm for infinite-time task scheduling in IaaS using MC with continuous parameters to search for an optimal solution is proposed, and a prototype is realised based on the designed model. Comparison of this prototype with a group of working models confirms the usefulness of the project.

The article is organized as follows. In the next section, an analytical representation of the researched object is presented using a Data Flow Diagram (DFD) and a mathematical description of the applied approach based on Markov Chain (MC). A third section is devoted to the implementation of model experiments, and a discussion of the experimental results is made in section 4.

2. Materials and Methods

The right to private life and its inviolability ("right to privacy") are directly related to the procedures for Personal Data Protection (PDP), which is an internationally recognized right, based on the understanding that personal data is the property of the person (Data Subject). As stated, the expansion of network communications and the growing possibilities of remote access to distributed information resources impose increasingly strict requirements on the applied information security policies. The globalization of public processes, the socialization of communications and the using cloud services create challenges to ensuring a reliable PDP. Cloud service providers emphasize the advantages of the cloud, mainly related to cost reduction, but the process of protecting information is not one of the main objects of discussion. Possible problems in providing personal data determine a high rate of distrust of users towards digitalization of services (over 70%). In particular, for cloud services, this is associated with basic features such as multi-tenancy, storing copies of data in different places in the virtual environment, applying common and standard security approaches, etc. In addition, a study by the Computer Security Institute shows that a fairly high share (more than 55%) when information security is compromised is due to accidental errors by staff, which necessitates paying attention to internal procedures for countering potential threats when processing personal data.

The classical organization of computer data processing takes place in an environment with a discrete structure, but the supported processes are probabilistic in nature. This allows both deterministic and probabilistic means to be used for preliminary formalization of processes. One possibility for a deterministic description is through the State Transition Network (STN), which allows to study the possible developments of the processes by analysing the paths "from beginning to end". In this direction is also the application of the Data Flow Diagram (DFD) for formal description of the movement of data flows in a given structure with an indication of the important places for their communication with other processes and objects. This has been applied to formalize the structural organization when conducting the research, taking into account the peculiarities and requirements of the PDP procedures.

The application of the probabilistic (stochastic) approach is often based on Markov processes, and when modelling computer data processing, the apparatus of Markov chains is suitable, because they are used to describe the probabilistic transitions between discrete states in determinate moments of time. The preliminary formalization in this case requires defining a finite set of states $S=\{s_1, \ldots, s_n\}$ for the studied process and a matrix of transition probabilities between the states $p_{ij} = P(s_i \rightarrow s_j)$. Stochastic analysis examines the sequence of states $<S(0), S(1),\ldots, S(k)>$, in which the MC falls, for which it is necessary to define a vector of initial probabilities for the formation of the initial state $S(0)=S(k=0)$. It is usually assumed that the process starts from the first state $s_1 \in S$, i.e. $P_0=\{1, 0, \ldots, 0\}$. Starting from the initial state, for each successive step $k=1, 2, \ldots$ of the process development, the conditional probability of transition from current state s_i to next state s_j can be determined by $p_{ij}(k)=P[S(k)=s_j / S(k-1)=s_i]$ based on the full probability formula:

$$p_j(k) = \sum_{i=1}^{n} p_i(k-1).p_{ij}; j = 1 \div n \quad (150)$$

as well as to calculate the final probabilities $P(k\to\infty)$ of falling into a certain state by (151)

$$\lim_{k\to\infty} p_{ij}(k) = p_j . \quad (152)$$

To investigate the processes in the proposed technological environment s stochastic Markov models were designed, and for their study, the developed author's program function "MARKOV" in the APL2 language environment [17] was used. It allows to determine the vector of probabilities for the states $P(k)=\{p_1(k), \ldots, p_n(k)\}$ for successive steps, the number of which is set by the user. After starting, it requires defining the main characteristics of the Markov chain: N – number of states; P[I,J] – the elements of the matrix of transition probabilities; PO[1÷N] – the elements of the vector of initial probabilities. A complete study can be organized through additional program functions "PATHS' and "ESTIMATES" [19], which together with "MARKOV", create a common program space for conducting analytical experiments in the APL2-environment. (153–162)

3. Preliminary Formalization (163)

The problems of data protection related to the growing threats of illegal access and their incorrect use are the subject of different documents, a basic example of which are the rules of conduct established in the USA and ensuring the necessary protection of information and corporate resources, known as SOX-rules , consolidated in the Sarbanes-Oxley Act of 2002. A study of the impact of these rules on the possible risk in resource management is done in [20] with an analysis of the situations before and after the adoption of these rules. Overall, the article highlights the positive impact of risk-reducing rules in resource management and increasing factor productivity and incentive compensation. (164–171)

In reality, it should be noted that the security of information resources requires the provision of adequate and functional security policies, which places specific requirements on Digital Right Management System (DRMS). Main trends are related to the inclusion of important components aimed at protecting personal data, for example: ✓ cryptographic algorithm for information encryption; ✓ cryptographic key management strategies; ✓ access control methods; ✓ methods and means for user identification and authentication; ✓ information content management with provenance verification and data copy control. At the heart of any DRMS are two processes - authentication and authorization, with which to prove that the specific information is used by the one who has pre-set rights to access it and all his actions can be tracked and checked, as well as what means of access is used. In this regard, all currently used technologies for authentication, and especially biometrics, become important for the reliable management of access to information resources. (172–183)

According to the regulatory documents, PDP means any action related to them – collection, storage, updating, correction, provision to a third party or transfer to another country, archiving, destruction, etc. All these processes must be carried out under strict organizational and technological measures to protect the means of storing personal data (Personal Data Registers – PDR). Formalization of the classical version of personal data processing in a centralized corporate system is presented in Figure 1 by using DFD with 5 external entities (source/receiver), 9 basic information procedures and 3 storage units. Part of the Information Security System (ISS) is the maintenance of a log (audit) file for access and activities carried out with the PDR (184–192)

A modification of a centralized environment could be made by transferring certain activities, including the storage of personal profiles with personal data to the cloud. This leads to the modification of the formalized description as well, introducing a generalized process "5C", uniting the undertaking of the activities of archiving, updating and deleting personal data with the maintenance of the stored arrays and profiles in data centres. Modified DFD-model of the decentralized structure is shown in Figure 2. The introducing of (193–198)

the new general process requires to actualize the role of the processes which are transferred in cloud and this is marked in DFD by "*" (6*, 8*, 9*). In addition, the new version requires duplication of procedures for ensuring information protection (identification, registration, authentication, authorization) with partial transfer to the cloud

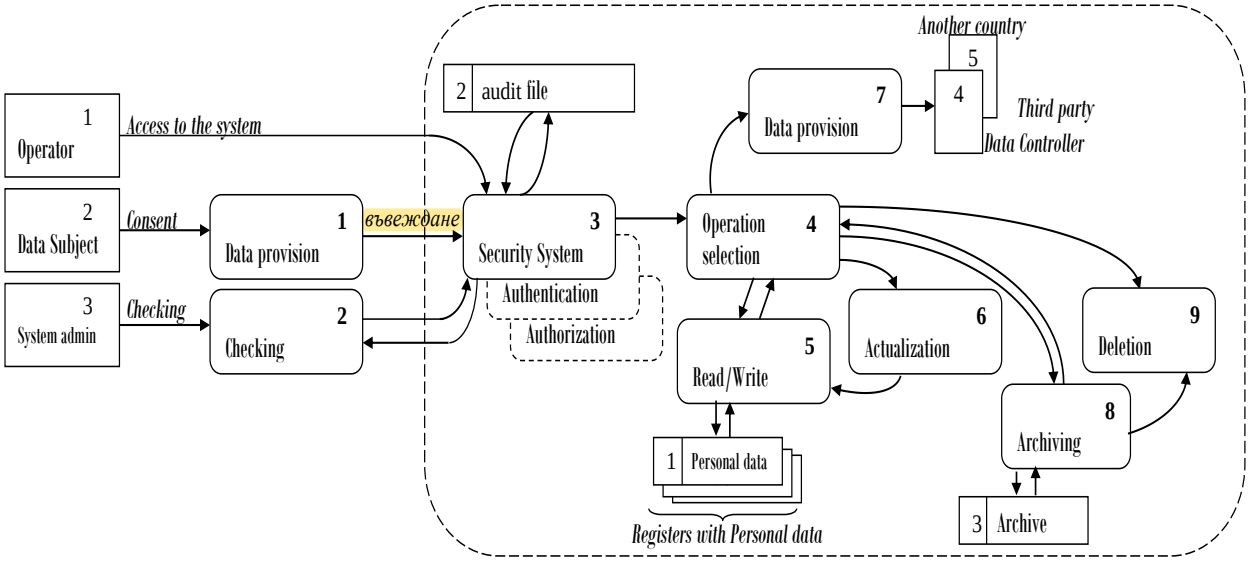

Figure 1. Formalization of personal data processing by using Data Flow Diagram (DFD)

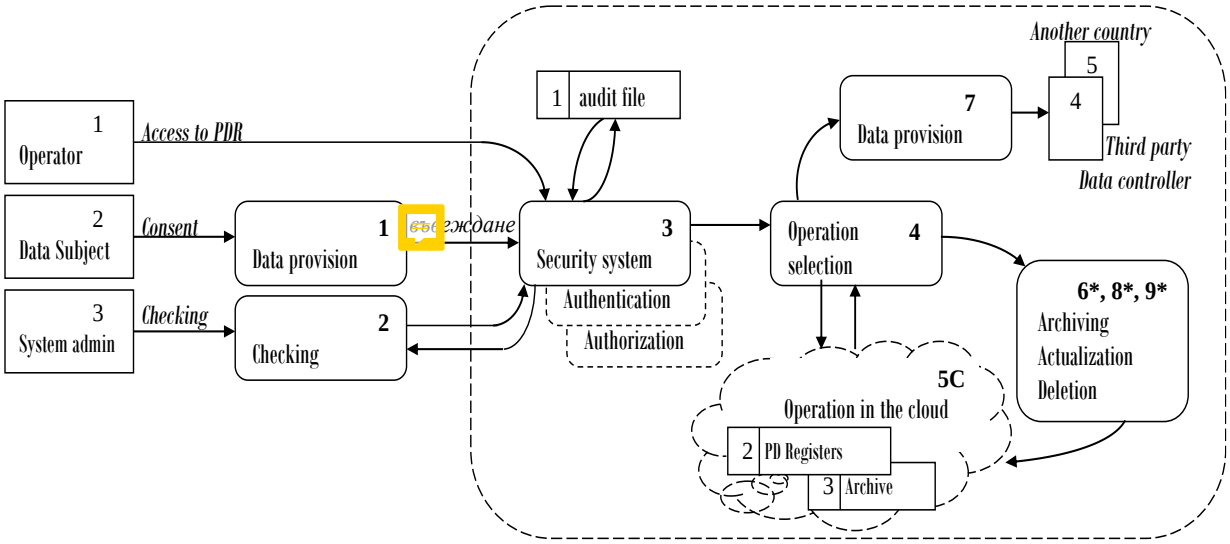

Figure 2. Modified DFD presenting processing of personal data in cloud

4. Stochastic Model Investigation

To conduct a model investigation, two models have been defined and solved using MC for the two formal DFD-descriptions presented in the previous section, respectively of traditional and "cloud" PDP. It is assumed that any random process, regardless of the source of a submitted request, begins with access to internal ISS funds, the basis for this assumption being the nature of the PD provisioning procedures by the individual.

4.1. Analytical investigation of traditional PDP

The Markov model for a traditional PDP presented in the Table 1 is defined on the base of the assumption made for the start of processes and selection of typical for the real traditional PDP values for the transition probabilities. The visual presentation of the MC graph of states is shown in Figure 3 with the following states:

s_1 – verification of the legitimacy of the request through authentication and authorization;

s_2 – selection of operation when access is allowed from the internal ISS;

s_3 – write/read to PDR;

s_4 – PD update in registry;

s_5 – provision of PD to a third party, another Data Controller or sending abroad;

s_6 – archiving of PD in the presence of a legal requirement for this;

s_7 – destruction of PD after fulfilling the purpose for which they were collected.

Table 1. Definition of the designed Markov model

Set of states:	$S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7\}$						
Vector of initial probabilities	$P_0 = \{1,0,0,0,0,0,0\}$						
{pij}	**s1**	**s2**	**s3**	**s4**	**s5**	**s6**	**s7**
s1	0,2	0,8	0	0	0	0	0
s2	0	0	0,4	0,2	0,2	0,1	0,1
s3	0	1	0	0	0	0	0
s4	0	0	1	0	0	0	0
s5	0	0	0	0	0	0	0
s6	0	0,3	0	0	0	0	0,7
s7	0	0	0	0	0	0	0

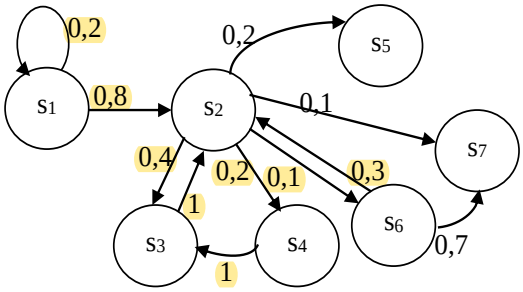

Figure 3. Markov model of traditional personal data processing (model "A").

The analytical definition of a model as a system of probabilities is as follows:

$$\begin{cases} p_1 = 0{,}2\,p_1 \\ p_2 = 0{,}8\,p_1 + p_3 + 0{,}3\,p_6 \\ p_3 = 0{,}4\,p_2 + p_4 \\ p_4 = 0{,}2\,p_2 \\ p_5 = 0{,}2\,p_2 \\ p_6 = 0{,}1\,p_2 \\ p_7 = 0{,}1\,p_2 + 0{,}7\,p_6 \\ \sum_{i=1}^{7} p_i = 1 \end{cases}$$

One solution to the system of probability equations is to represent the probabilities by one of them, e.g. p_2, and next substituting into the last equation.

$$p_1 = \frac{0{,}37}{0{,}8} p_2 = 0{,}4625 p_2;$$

$$p_3 = 0{,}6 p_2; \quad p_4 = p_5 = 0{,}2 p_2;$$

$$p_6 = 0{,}1 p_2; \quad p_7 = 0{,}27 p_2$$

$$\rightarrow (0{,}4625 + 1 + 0{,}6 + 0{,}2 + 0{,}2 + 0{,}1 + 0{,}27) p_2 = 1$$

After solving the last equation and substituting into the expressions, the following estimates are formed for the final probabilities of falling into each of the states:

$$p_1 = 0{,}165; \quad p_2 = 0{,}353; \quad p_3 = 0{,}212; \quad p_4 = 0{,}071$$

$$p_5 = 0{,}071; \quad p_6 = 0{,}035; \quad p_7 = 0{,}095$$

4.2. Analytical investigation of "cloud" PDP

The Markov model for "cloud" PDP (Figure 4) is a modification of the previous one and corresponds to the processes from the DFD (Figure 2). A generalized state s_C is created, replacing states s_3, s_6 and s_7, whose activities are taken over by cloud services.

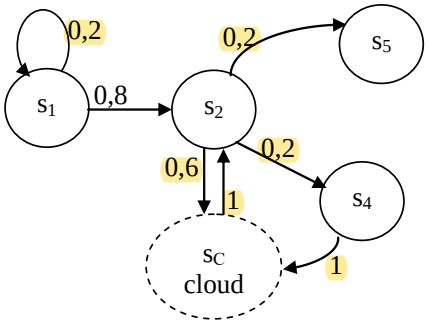

Figure 4. Markov model of "cloud" PDP (model "C").

Since updating is a process of incoming new (or corrected) PDs for an individual and receiving them from a Data Controller operator (employee), the s_4 state activity cannot be migrated to the cloud. The same applies to the process of providing PD, as it is related to certain regulatory requirements. The analytical Markov model notation for the situation is as follows:

$$\begin{cases} p_1 = 0{,}2 p_1 \\ p_2 = 0{,}8 p_1 + p_C \\ p_4 = 0{,}2 p_2 \\ p_5 = 0{,}2 p_2 \\ p_C = 0{,}6 p_2 + p_4 \\ p_1 + p_2 + p_4 + p_5 + p_C = 1 \end{cases}$$

After solving the system of probabilistic equations, the following estimates for the final probabilities are determined:

$$p_1 = 0{,}102; \quad p_2 = 0{,}408; \quad p_4 = 0{,}082$$

$$p_5 = 0{,}082; \quad p_C = 0{,}326$$

4.3. Experimental results discussion

The diagram in Figure 5 presents a visual summarization of the obtained analytical results for model "A", allowing easy comparison of the probabilities of falling into the separate states. It can be seen that the load of the states related to the selection operations

of relevant data processing activities and operation with the registry system for their storage is the greatest.

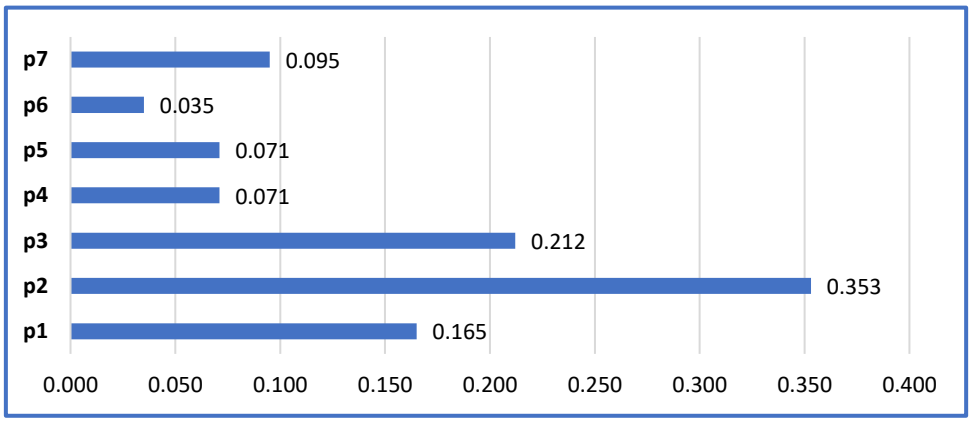

Figure 5. Graphical visualization of analytical assessments for the states of Model "A"

A joint visualization of the analytical results of solutions of the two models is made in figure 6, where the probabilities of performing the corresponding activities in steady state are presented. The comparative analysis shows non-significant differences in the marginal probability values for the two situations (the two models), but model B (the cloud option) having a certain advantage for the main PDP fulfilment activities related to the responsibilities of the Data Controller employees (Data Operators). This confirms the high importance of complying with legal requirements and ensuring strict internal rules in the relevant institution

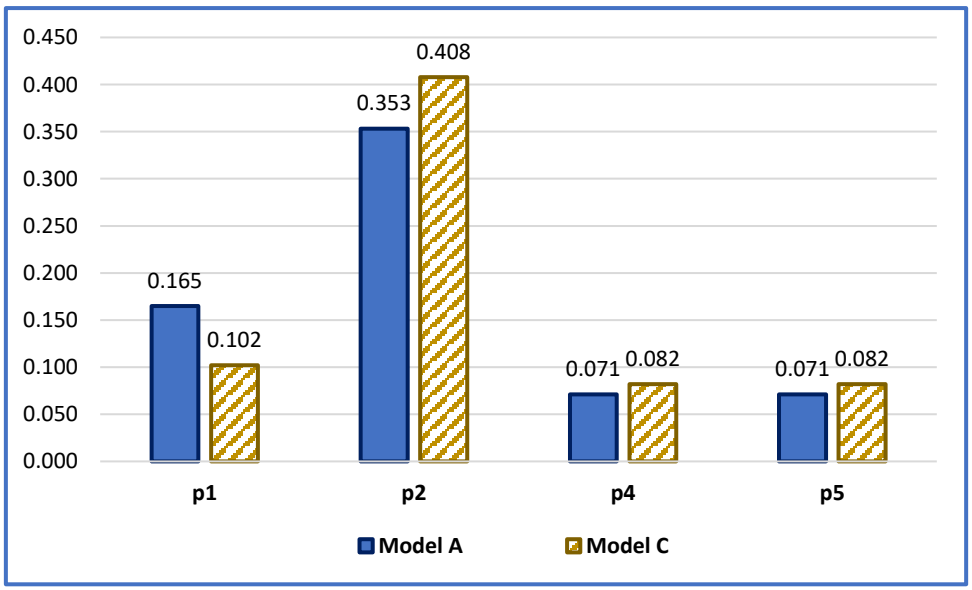

Figure 6. Comparison of basic activities for the two models

On the other hand, however, it should be emphasized that moving some PDP activities to the cloud has a certain effect, observing a certain reduction in the level of employment in certain states (DFD processes). This can be seen from the joint presentation of the transferred activities in the two models "A" and "C" from Figure 7.

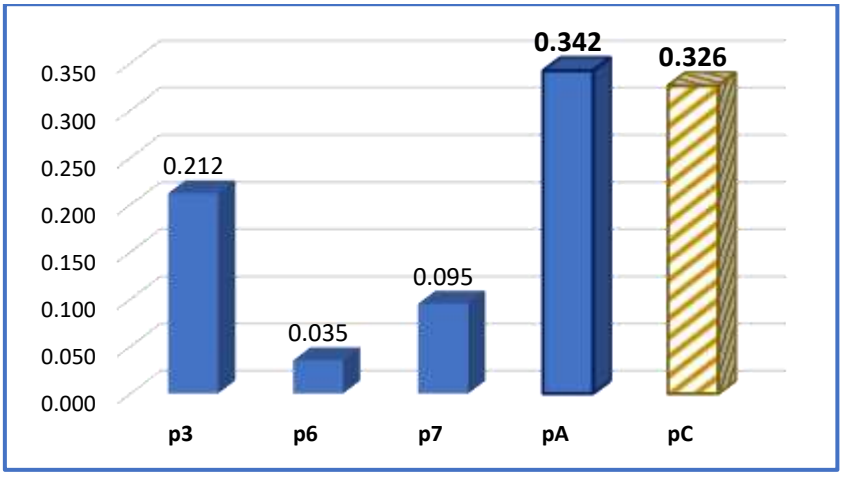

Figure 7. Equivalence of assessments before and after moving activities to the cloud (**p**$_A$ = p$_3$ + p$_6$ + p$_7$ for model "A"; **p**$_c$ for model "C")

Although moving certain process activities (6*, 8* and 9* of DFD - figure 2) to the cloud eases the workload of ISS service operators, this does not change the responsibility of the Data Controller and the requirements to ensure internal rules for identification and access management. Due to the fact that standard data protection mechanisms are traditionally applied in the cloud, the use of data centres and cloud services should only take place after providing serious guarantees for ensuring adequate data protection related to access management and authorization, authentication, maintenance of audit information, implementation of architectural requirements for the cloud platform, etc. In this sense, the patent from [12] can provide the necessary level of security when processing personal data in a distributed environment. One solution is to define authorization in depth, implemented at three levels: high level – for meta-level management of access to applications and resources; middle level – for data level access control; low level – to control functions with specific data.

5. Conclusion

The main purpose of the article is to present a point of view for transferring certain personal data processing activities to a cloud environment using data centres (data warehouses) and the virtual environment of the cloud for multiple communication. The main problem for discussion is the implementation of adequate procedures for information security in the organization of a heterogeneous environment for maintaining information resources, and the article specifically discusses the organization of the system for ensuring reliable protection of profiles with personal data. The relevance of this problem is confirmed by the continuous development of digital technologies, which creates challenges for personal privacy [21]. In practice, this is one stage of the overall development and investigation of the heterogeneous environment, where a stochastic approach is applied to further validate the effectiveness of the planned PDP procedures.

The main contribution is the formalization of the personal data processing by using the DFD apparatus and the analytical development of the presented stochastic models, allowing to make a comparison of the features of the processes supported in the traditional and in the cloud version. From the conducted model investigation and analysis of the obtained estimates in the case of stationary processes, it can be seen that regarding the obligations of the Data Controller there is no significant difference between the relative weights of the two options. At the same time, both models maintain the importance of authorization and authentication as information security processes. This confirms the need to build a serious ISS with specific measures to protect PDR, meeting clearly defined rules and responsibilities when working with cloud resources. Such a cloud platform should provide the following capabilities: ✓ integrity of stored user data; ✓ preventing

unauthorized access to personal data; ✓ maintaining complete information about every attempt to access personal data; ✓ possibility of easy verification by the user whether the PDP policy is followed; ✓ possibility of efficient and secure processing of sensitive personal data;

Funding: This research received no external funding

Data Availability Statement: Not applicable.

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

References

1. Hilbert, M. Digital technology and social change: the digital transformation of society from a historical perspective, *Dialogues in Clinical Neuroscience* **2020**, *Vol. 22*, No. 2, pp.189-194, DOI: 10.31887/DCNS.2020.22.2/mhilbert
2. Gregory, R.W.; Henfridsson, O.; Kaganer, E.; Kyriakou, H. Data network effects: Key conditions, shared data, and the data value duality. Academy of Management review **2022**, *Vol. 47*, No.1, pp.189-192 (https://doi.org/10.5465/amr.2021.0111)
3. Halili, M.K.; Cico, B. SLA management for comprehensive virtual machine migration considering scheduling and load balancing algorithm in cloud data centers. *International Journal on Information Technologies and Security* **2020**, *Vol. 12*, No. 4, pp. 23-34.
4. Williamson, J.R.; O'Hagan, J.; Guerra-Gomez, J.A; Williamson, J.H.; Cesar, P.; Shamma, D.A. Digital proxemics: Designing social and collaborative interaction in virtual environments. In Proceedings of *CHI'22 Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* **April 2022**, art. No. 423, pp. 1-12 (https://doi.org/10.1145/3491102.3517594).
5. Qian,X.; Chen, H.; Cai, Y.; Chu, K.-C.; Xu, W.; Huang, M.-C. Transfer learning model knowledge across multi-sensors locations over body sensor network. *IEEE Sensors Journal* **2022**, *Vol. 22*, No. 11, pp. 10663-10670. doi: 10.1109/JSEN.2022.3166187
6. Trnka, M.; Abdelfattah, A.S.; Shrestha, A.; Coffey, M.; Cerny, T. Systematic review of authentication and authorization advancements for the Internet of Things. *Sensors* **2022**, *Vol. 22*, No. 4, p.1361.
7. de Almeida, M.G.; Canedo, E.D. Authentication and authorization in microservices architecture: A systematic literature review. *Applied Sciences* **2022**, *Vol. 12*, No. 66, p.3023 (https://doi.org/10.3390/app12063023).
8. Bhattacharjya, A. A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication. *International Journal of Applied Mathematics and Computer Science* **2022**, *Vol. 32*, No. 3, pp.403-413.
9. Alshathri, S.; Alrashidi, E.; Albawardi, N.; Almojel, H.; Jamail, N.S.M. Improvement of the CIA triad for Al-Rajhi online banking system. In Proceedings of the 5th Int'l Conf. of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 3 May 2022, pp. 67-69, doi: 10.1109/WiDS-PSU54548.2022.00025.
10. Swain, S.R.; Singh, A.K.; Lee, C.N. Efficient resource management in cloud environment. *arXiv:2207.12085 (Distributed, Parallel, and Cluster Computing)* **2022**, https://doi.org/10.48550/arXiv.2207.12085
11. Yang, M.; Gao, T.; Xie, W.; Jia, L.; Zhang, T. The assessment of cloud service trustworthiness state based on DS theory and Markov chain. *IEEE Access* **2022**, *Vol. 10*, No. pp.68618-68632. **DOI:** 10.1109/ACCESS.2022.3185684
12. Balasubramanian, V.A.; Kulasekaran, R.; Subramanian, V. *Data protection as a service* **28 April 2022**, U.S. Patent Application 17/077,571.
13. Oleinikova, S.A.; Selishchev, I.A.; Kravets,O.Ja.; Rahman, P.A.; Aksenov, I.A.. Simulation model for calculating the probabilistic and temporal characteristics of the project and the risks of its untimely completion, *International Journal on Information Technologies and Security* **2021**, *Vol. 13*, No. 2, pp. 55-62.
14. Digalovski, M.; Rafajlovski, G. Distribution transformer mathematical model for power losses minimization. *International Journal on Information Technologies and Security* **2020**. *Vol. 12*, No. 2, pp. 57-68
15. Hagemann, P.; Hertrich, J.; Steidl, G. Stochastic normalizing flows for inverse problems: a Markov Chains viewpoint. *SIAM/ASA Journal on Uncertainty Quantification* **2022**, *Vol. 10*, No. 3, pp.1162-1190.
16. Jones, G.L.; Qin, Q. Markov chain Monte Carlo in practice. *Annual Review of Statistics and Its Application* **2022**, *Vol. 9*, No. 1, March, pp.557-578.
17. Romansky, R. An approach for program investigation of computer processes presented by Markov models. *International Journal on Information Technologies and Security* **2022**, *Vol. 14*, No. 4, pp. 45-54.
18. Nithiyanandam, N.; Rajesh, M.; Sitharthan, R.; Shanmuga Sundar, D.; Vengatesan, K.; Madurakavi, K. Optimization of performance and scalability measures across cloud based IoT applications with efficient scheduling approach. *International Journal of Wireless Information Networks* **2022**, *Vol. 29*, pp.1-12 (https://doi.org/10.1007/s10776-022-00568-5)
19. Romansky, R. Mathematical Modelling and Study of Stochastic Parameters of Computer Data Processing. *Mathematics* **2021**, *Vol. 9*, No. 18, art. 2240. DOI: 10.3390/math9182240
20. Hillier, D.; McColgan, P.; Tsekeris, A. How did the Sarbanes–Oxley Act affect managerial incentives? Evidence from corporate acquisitions. *Review of Quantative Finance and Accounting* **2022**, *Vol. 58*, pp.1395–1450. https://doi.org/10.1007/s11156-021-01028-6
21. Romansky, R., Noninska, I. Challenges of the Digital Age for privacy and personal data protection. *Mathematical Biosciences and Engineering* **2020**, *Vol. 17*, No. 5, pp.5288-5303 (article MBE2020268), DOI: 10.3934/mbe.2020286