axioms

MDPI

Article

Mathematical Model Investigation of a Technological Structure for Personal Data Protection

Radi Romansky

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

Abstract: The contemporary digital age is characterized by the massive use of different information technologies and services in the cloud. This raises the following question: "Are personal data processed correctly in global environments?" It is known that there are many requirements that the Data Controller must perform. For this reason, this article presents a point of view for transferring some activities for personal data processing from a traditional system to a cloud environment. The main goal is to investigate the differences between the two versions of data processing. To achieve this goal, a preliminary deterministic formalization of the two cases using a Data Flow Diagram is made. The second phase is the organization of a mathematical (stochastic) model investigation on the basis of a Markov chain apparatus. Analytical models are designed, and their solutions are determined. The final probabilities for important states are determined based on an analytical calculation, and the higher values for the traditional version are defined for data processing in registers ("2": access for write/read −0.353; "3": personal data updating −0.212). The investigation of the situations based on cloud computing determines the increasing probability to be "2". Discussion of the obtained assessment based on a graphical presentation of the analytical results is presented, which permits us to show the differences between the final probabilities for the states in the two versions of personal data processing.

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

MSC: 37M21

check for updates

Citation: Romansky, R. Mathematical Model Investigation of a Technological Structure for Personal Data Protection. *Axioms* **2023**, *12*, 102. https://doi.org/10.3390/axioms12020102

Academic Editors: Cheng-Shian Lin, Chien-Chang Chen and Yi-Hsien Wang

Received: 31 December 2022
Revised: 13 January 2023
Accepted: 13 January 2023
Published: 18 January 2023

Copyright: © 2023 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 (InSoc) is characterized by the massive informatization and penetration of digital technologies in all areas. This is described in [1] as "*the most recent long wave of humanity's socioeconomic evolution*", with an emphasis on the fact 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, which has a reflection on the efficiency of the data network [2] due to the increased access to remote resources and use of cloud data centers [3], data sharing in virtual environments [4], Internet of Things (IoT), including the sensor collection of personal data [5], and others. For example, the previously cited article confirms that today's advanced sensor technologies "*generate a large amount of valuable data*" for different applications, such as "*health care, elderly protection, human activity abnormal detection, and surveillance*". One result of technologies in the digital space is the dissemination of personal data (freely or unknowingly), which raises a serious question concerning 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 adopted. A basic requirement should be countermeasures against the 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 for regulating the access to and use of objects and data is discussed in [7], where it is emphasized that building systems with multiple services increases the security impact when compared with the monolithic style. In order to answer important security questions in complex environments, a systematic review of the main challenges when using mechanisms and technologies for authentication and authorization in micro-services is performed.

The purpose of this article is to present a point of view on the technological organization of personal data protection processes in an example environment (administrative system) that uses cloud services and data centers and applies the requirements of the CIA (Confidentiality, Integrity, Availability) triad. 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 the IoT and cyber physical systems (CPS) is presented in [8], and a solution involving blockchain technology is proposed with an analysis of the similarities and differences. Another study "*on the improvement of CIA triad to reduce the risk on online banking system*" is presented in [9].

Cloud computing allows us to take 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 one's own assets are reduced. For the user, the "cloud" is a virtual environment for data processing and storage. The services offered provide various cloud capabilities, requiring the 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 of 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 directions. Another study [11] discusses how cloud service reliability should be further evaluated in specific conditions and proposes an approach based on combining cloud service reliability indicators to obtain an effective evaluation and improve data security. Despite cloud service providers' claims of good information security at the platform level, doubts have been 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 data protection policy using the machine-learning model and comparisons with previous instructions [12].

When researching processes developing in a computer environment, as well as for organizing structures, various possibilities are applied, such as benchmark and synthetic workload; monitoring through hardware, software, and combined means; computer modeling (abstract, functional, analytical, simulation, empirical); as well as statistical analysis of empirical data. Each of these approaches has its advantages and peculiarities, and the use of each of them depends on the researched object and the set tasks.

One of the applied approaches when researching processes in various systems and applications is modeling based on an appropriate apparatus and instrumentation. For example, simulation modeling is applied in [13] to study the probabilistic behavior and timing characteristics of interdependent tasks of arbitrary durations. 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 is 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 the parameters of the transformer 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 indicates Markov processes and, in particular, Markov chains (MC) to be 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 the approach is combined with the Monte Carlo method for assessing the characteristics of

probability distributions and a review of the "*methods for assessing the reliability of the simulation effort, with an emphasis on those most useful in practically relevant settings*" is performed. 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 by applying the apparatus of Markov chains (MC). The choice of 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, as developed in the APL2 language [17], is used and a graphic interpretation of the evaluations is 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 the IoT 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 realized based on the designed model. A comparison of this prototype with a group of working models confirms the usefulness of the project.

This 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 the Markov Chain (MC). The third section is devoted to the implementation of the model experiments, and a discussion of the experimental results is presented in Section 4.

2. Materials and Methods

The right to a 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 are 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 use of cloud services pose challenges to ensuring reliable PDP. Cloud service providers emphasize the advantages of the cloud, mainly those related to cost reduction, but the process of protecting information is not one of the main objects of discussion. Possible problems when providing personal data determine a high rate of distrust among users toward the 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%) of compromised information security 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, although the supported processes are probabilistic in nature. This allows both deterministic and probabilistic means to be used for the preliminary formalization of processes. One possibility for a deterministic description involves the State Transition Network (STN), which allows us to study the possible developments of the processes by analyzing the paths "from beginning to end". In this direction is also the application of a Data Flow Diagram (DFD) for the 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 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 modeling 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 the definition of a finite set of states $S = \{s_1, \ldots, s_n\}$ for the studied process and a matrix of transition probabilities between those 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 the 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 a transition from the current state s_i to the 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 (1):

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

which can also be used to calculate the final probabilities $P(k \rightarrow \infty)$ of falling into a certain state by

$$\lim_{k \rightarrow \infty} p_{ij}(k) = p_j.$$

To investigate the processes in the proposed technological environment, s stochastic Markov models are designed, and for their study, the developed author's program function "MARKOV" in the APL2 language environment [17] is used. This allows us to determine the vector of the 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 the definition of the main characteristics of the Markov chain: N—number of states; P[I,J]—the elements of the matrix of transition probabilities; and PO [1 ÷ N]—the elements of the vector of initial probabilities. A complete study can be organized through the additional program functions "PATHS' and "ESTIMATES" [19], which, together with "MARKOV", create a common program space for conducting analytical experiments in the APL2 environment.

3. Preliminary Formalization

The problems of data protection related to the growing threats of illegal access and incorrect use are the subject of different documents. A basic example here are the rules of conduct established in the USA to ensure the necessary protection of information and corporate resources, which are known as the SOX rules, as 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 on resource management and increasing factor productivity and incentive compensation.

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

According to regulatory documents, PDP refers to any action related to them—collection, storage, updating, correction, provision to a third party, 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]). The formalization of the classical version of personal data processing in a centralized corporate

system is presented in Figure 1 by using a DFD with five external entities (source/receiver), nine basic information procedures, and three 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.

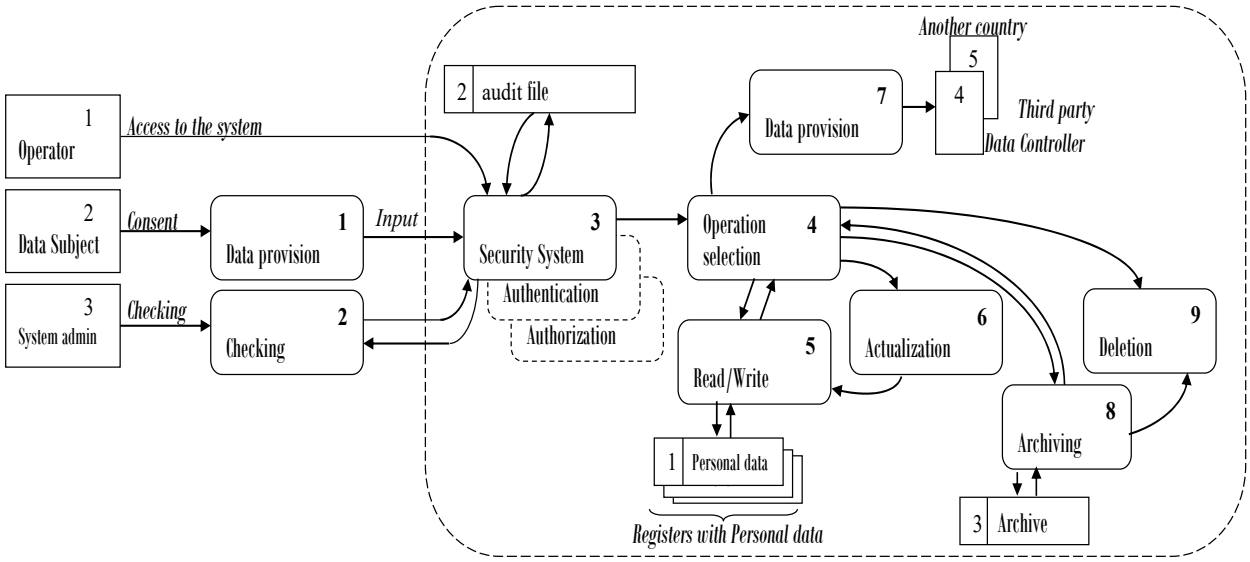

Figure 1. Formalization of personal data processing using a Data Flow Diagram (DFD).

A modification to a centralized environment can 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", thereby uniting the undertaking of the activities of archiving, updating, and deleting personal data with the maintenance of the stored arrays and profiles in data centers. The modified DFD model of the decentralized structure is shown in Figure 2. The introduction of the new general process requires actualizing the role of the processes that are transferred to the cloud, which this is marked in the DFD by "*" (6 *, 8 *, 9 *). In addition, the new version requires the duplication of procedures for ensuring information protection (identification, registration, authentication, authorization) with partial transfer to the cloud.

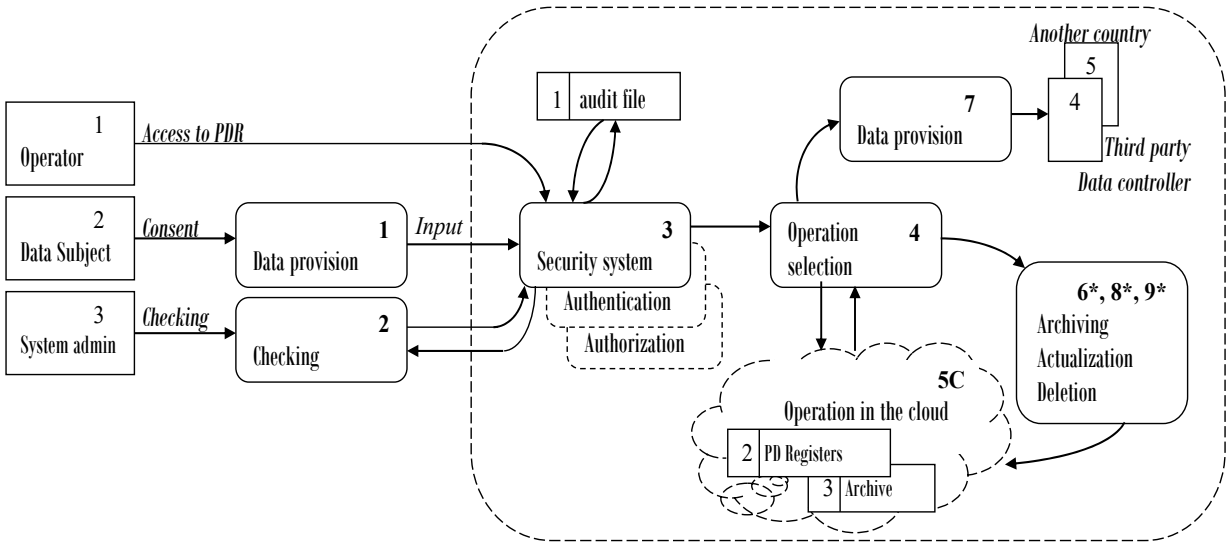

Figure 2. Modified DFD presenting the processing of personal data in the cloud.

4. Stochastic Model Investigation

To conduct the model investigation, two models are defined and solved using MC for the two formal DFD descriptions presented in the previous section: 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 is the nature of the PD provisioning procedures by the individual.

4.1. Analytical Investigation of Traditional PDP

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

Table 1. Definition of the designed Markov model.

Set of States: Vector of Initial Probabilities				$S = \{s_1,s_2,s_3,s_4,s_5,s_6,s_7\}$ $P_0 = \{1,0,0,0,0,0,0\}$			
$\{p_{ij}\}$	s_1	s_2	s_3	s_4	s_5	s_6	s_7
s_1	0.2	0.8	0	0	0	0	0
s_2	0	0	0.4	0.2	0.2	0.1	0.1
s_3	0	1	0	0	0	0	0
s_4	0	0	1	0	0	0	0
s_5	0	0	0	0	0	0	0
s_6	0	0.3	0	0	0	0	0.7
s_7	0	0	0	0	0	0	0

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.

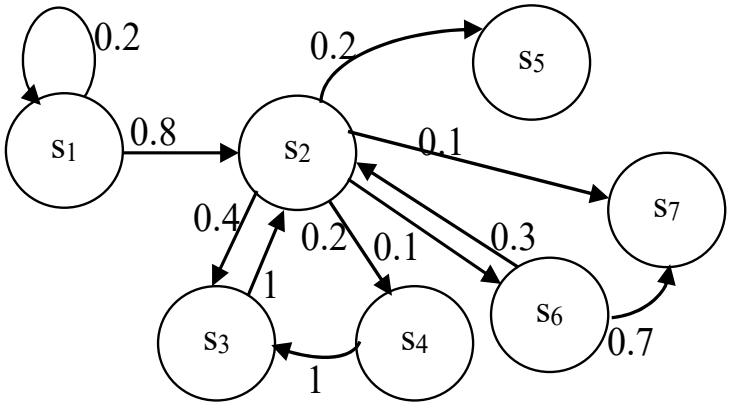

Figure 3. Markov model of traditional personal data processing (model "A").

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

$$
\begin{aligned}
p_1 &= 0.2p_1 \\
p_2 &= 0.8p_1 + p_3 + 0.3p_6 \\
p_2 &= 0.8p_1 + p_3 + 0.3p_6 \\
p_3 &= 0.4p_2 + p_4 \\
p_4 &= 0.2p_2 \\
p_5 &= 0.2p_2 \\
p_6 &= 0.1p_2 \\
p_7 &= 0.1p_2 + 0.7p_6 \\
\sum_{i=1}^{7} p_i &= 1
\end{aligned}
$$

One possible solution to the presented system of probability permits us to calculate the values for all the final probabilities as follows:

$$p_1 = \frac{0.37}{0.8} p_2 = 0.4625p_2;\ p_3 = 0.6p_2;\ p_4 = p_5 = 0.2p_2;\ p_6 = 0.1p_2;\ p_7 = 0.27p_2$$

This permits us to construct Equation (2) for the calculation of the value of the final probability p_2.

$$(0.4625 + 1 + 0.6 + 0.2 + 0.2 + 0.1 + 0.27)p_2 = 1 \quad (2)$$

After solving Equation (2) and substituting it into the expressions, the following estimates are formed for the final probabilities of falling into each of the states:

$$p_1 = 0.165;\ p_2 = 0.353;\ p_3 = 0.212;\ p_4 = p_5 = 0.071;\ p_6 = 0.035;\ p_7 = 0.095$$

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.

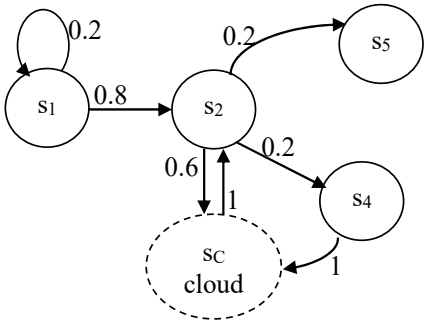

Figure 4. Markov model of "cloud" PDP (model "C").

As updating is a process involving 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 this situation is as follows:

$$
\begin{aligned}
p_1 &= 0.2p_1 \\
p_2 &= 0.8p_1 + p_C \\
p_4 &= 0.2p_2 \\
p_4 &= 0.2p_2 \\
p_C &= 0.6p_2 + p_4 \\
p_1 + p_2 + p_4 + p_5 + p_C &= 1
\end{aligned}
$$

After solving the system of probabilistic equations, the following estimates for the final probabilities are determined: $p_1 = 0.102$; $p_2 = 0.408$; $p_4 = 0.082$; $p_5 = 0.082$; and $p_C = 0.326$.

4.3. Experimental Results Discussion

The diagram in Figure 5 presents a visual summarization of the obtained analytical results for model "A", allowing for 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.

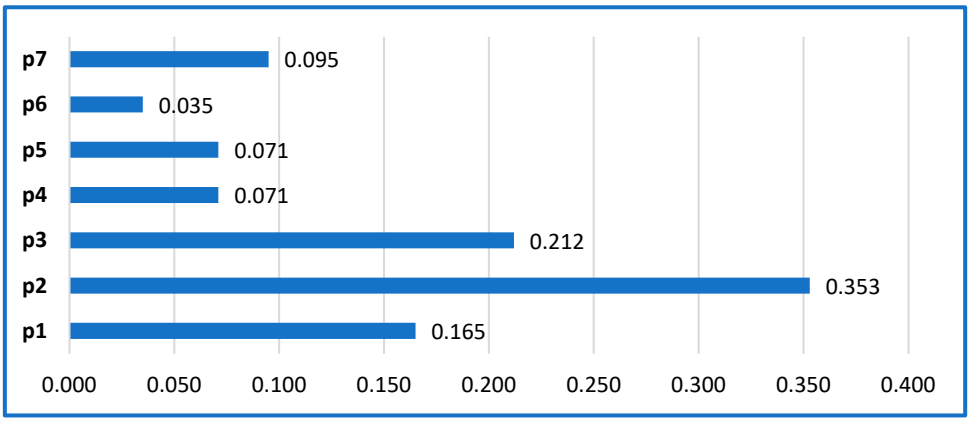

Figure 5. Graphical visualization of analytical assessments for the states of Model "A".

A joint visualization of the analytical results of the solutions for the two models is presented in Figure 6, where the probabilities of performing the corresponding activities in a steady state are presented. The comparative analysis shows non-significant differences in the marginal probability values for the two situations (the two models), although model "B" (the cloud option) has a certain advantage for the main PDP fulfillment 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.

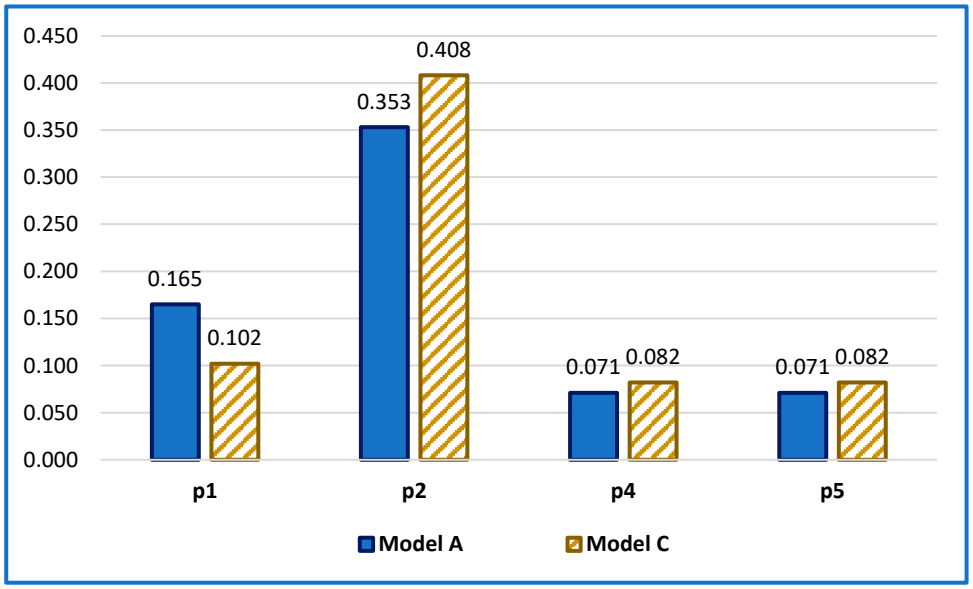

Figure 6. Comparison of basic activities for the two models.

On the other hand, it should be emphasized that moving some PDP activities to the cloud has a certain effect, leading to 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", in Figure 7.

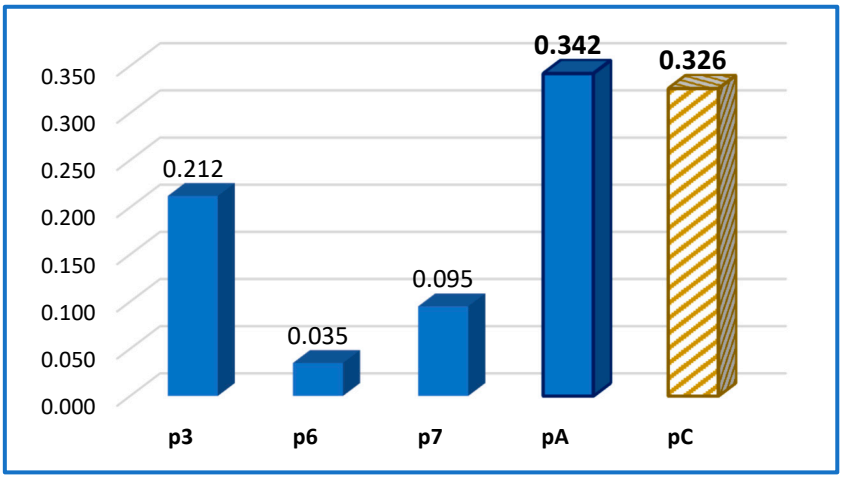

Figure 7. Equivalence of assessments before and after moving activities to the cloud ($p_A = p_3 + p_6 + p_7$ for model "A"; p_c for model "C").

Although moving certain process activities (6 *, 8 *, and 9 * of DFD [Figure 2]) to the cloud eases the workload of ISS service operators, it does not change the responsibility of the Data Controller or the requirement 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 centers and cloud services should only take place after providing serious guarantees for ensuring adequate data protection related to access management, 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 and implement it at three levels: high level—for meta-level management of access to applications and resources; middle level—for data level access control; and low level—to control functions with specific data.

5. Conclusions

The main purpose of this article is to present a point of view for transferring certain personal data processing activities to a cloud environment using data centers (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. This article specifically discusses the organization of a system for ensuring the 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 personal data processing using the DFD apparatus and the analytical development of the presented stochastic models, allowing us to make a comparison of the features of the processes supported in the traditional and cloud versions. 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, which must meet 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 as to whether the PDP policy is followed; and ✓ possibility of efficient and secure processing of sensitive personal data.

The obtained results of this research provide an idea of the relevance of the processes in the two selected implementation options, and the goal is to determine the effectiveness of the application of cloud services. They can be used in the selection of specific techniques and means, mainly in the organization of the security of access to personal data, as well as in the implementation of heterogeneous systems, such as proposed in [22].

The research carried out allows for an extension in several directions defining future research, for example, an extension of the model study by applying deterministic means such as graph theory [23] and the Petri nets apparatus [22], as well as possibly simulation modeling of the main work processes with personal data, mainly in cloud services, with statistical analysis of the accumulated data from experiments [24].

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

CIA	Confidentiality, Integrity, Availability
CPS	Cyber Physical Systems
DFD	Data Flow Diagram
DRMS	Digital Rights Management System
InSoc	Information Society
IoT	Internet of Things
ISS	Information Security System
PD	Personal Data
PDP	Personal Data Protection
PDR	Persona Data Register
MC	Markov Chain
PM	Physical Machines
STN	State Transition Network
VM	Virtual Machines

References

1. Hilbert, M. Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues Clin. Neurosci.* **2020**, *22*, 189–194. [CrossRef] [PubMed]
2. Gregory, R.W.; Henfridsson, O.; Kaganer, E.; Kyriakou, H. Data network effects: Key conditions, shared data, and the data value duality. *Acad. Manag. Rev.* **2022**, *47*, 189–192. [CrossRef]
3. Halili, M.K.; Cico, B. SLA management for comprehensive virtual machine migration considering scheduling and load balancing algorithm in cloud data centers. *Int. J. Inf. Technol. Secur.* **2020**, *12*, 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 the CHI'22 Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April–2 May 2022; pp. 1–12. [CrossRef]
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 Sens. J.* **2022**, *22*, 10663–10670. [CrossRef]

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**, *22*, 1361. [CrossRef] [PubMed]
7. de Almeida, M.G.; Canedo, E.D. Authentication and authorization in microservices architecture: A systematic literature review. *Appl. Sci.* **2022**, *12*, 3023. [CrossRef]
8. Bhattacharjya, A. A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 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 International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 28–29 March 2022; pp. 67–69. [CrossRef]
10. Swain, S.R.; Singh, A.K.; Lee, C.N. Efficient Resource Management in Cloud Environment. *arXiv* **2022**, arXiv:2207.12085. Distributed, Parallel, and Cluster Computing. [CrossRef]
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**, *10*, 68618–68632. [CrossRef]
12. Balasubramanian, V.A.; Kulasekaran, R.; Subramanian, V. Data Protection as a Service. U.S. Patent 17/077,571, 28 April 2022.
13. Oleinikova, S.A.; Selishchev, I.A.; Kravets, O.J.; 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. *Int. J. Inf. Technol. Secur.* **2021**, *13*, 55–62.
14. Digalovski, M.; Rafajlovski, G. Distribution transformer mathematical model for power losses minimization. *Int. J. Inf. Technol. Secur.* **2020**, *12*, 57–68.
15. Hagemann, P.; Hertrich, J.; Steidl, G. Stochastic normalizing flows for inverse problems: A Markov Chains viewpoint. *SIAM/ASA J. Uncertain. Quantif.* **2022**, *10*, 1162–1190. [CrossRef]
16. Jones, G.L.; Qin, Q. Markov Chain Monte Carlo in Practice. *Annu. Rev. Stat. Its Appl.* **2022**, *9*, 557–578. [CrossRef]
17. Romansky, R. An approach for program investigation of computer processes presented by Markov models. *Int. J. Inf. Technol. Secur.* **2022**, *14*, 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. *Int. J. Wirel. Inf. Netw.* **2022**, *29*, 442–453. [CrossRef]
19. Romansky, R. Mathematical Modelling and Study of Stochastic Parameters of Computer Data Processing. *Mathematics* **2021**, *9*, 2240. [CrossRef]
20. Hillier, D.; McColgan, P.; Tsekeris, A. How did the Sarbanes–Oxley Act affect managerial incentives? Evidence from corporate acquisitions. *Rev. Quant. Finance Account.* **2022**, *58*, 1395–1450. [CrossRef]
21. Romansky, R.; Noninska, I. Challenges of the Digital Age for privacy and personal data protection. *Math. Biosci. Eng.* **2020**, *17*, 5288–5303. [CrossRef] [PubMed]
22. Romansky, R.; Noninska, I. Deterministic Model Investigation of Processes in a Heterogeneous e-Learning Environment. *Int. J. Hum. Cap. Inf. Technol. Prof.* **2022**, *13*, 28. [CrossRef]
23. Romansky, R. Formalization and Discrete Modelling of Communication in the Digital Age by Using Graph Theory. In *Handbook of Research on Advanced Applications of Graph Theory in Modern Society*; Pal, M., Samanta, S., Pal, A., Eds.; IGI Global: Hershey, PA, USA, 2020; Chapter 13; pp. 320–353. [CrossRef]
24. Romansky, R. Investigation of Network Communications by Using Statistical Processing of Monitored Data. In Proceedings of the 2022 IEEE International Conference on Information Technologies (InfoTech-2022), Varna, Bulgaria, 15–16 September 2022; pp. 37–40. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.