INFORMATION SECURITY MANAGEMENT FOR CLOUD INFRASTRUCTURE

A.V. Tsaregorodtsev[1], I. Ya. Lvovich[2], M. S. Shikhaliev[3], A. N. Zelenina[2], O. N. Choporov[4]

[1]Moscow State Linguistic University, [2]Voronezh Institute of High Technologies, [3]Russian University of Transport, [4]Voronezh State Technical University
e-mail: choporov_oleg@mail.ru
Russian Federation

Abstract: The advent of cloud computing foreshadows far-reaching plans for systems and networks of federal agencies, as well as other government organizations and business entities. Undoubtedly, the migration to the cloud computing architecture will allow organizations to reduce the total cost of implementing and supporting the infrastructure and reduce the time to develop new business applications. At the same time, many of the features that make cloud computing attractive can conflict with traditional information security models. In this case, the most pressing and current issue in the migration of data to the cloud will be the issue of information security. In this article particular attention is paid to open issues of information security and options for their solution when building an integrated information security system for information systems operating on the basis of cloud computing technology.

Key words: cloud computing, cloud services, information security threats, information security management methods, modelling, Petri net.

1. INTRODUCTION

Cloud computing in the near future will become one of the most common IT technologies for application deployment due to its key features: solution flexibility, availability on demand and a good price / quality ratio. Cloud computing will be understood as a model that allows universal and convenient access to a common pool of configurable computing resources on demand (for example, a set of networks, servers, data storages, applications and services) that can be promptly provided by a service provider [1].

The main purpose of building a secure architecture should be based on the principles of sufficiency of a certain level of protection of business assets of the organization. However, when analyzing complex business processes, it is very difficult to determine whether the subject's current authority to the object of access

is consistent with the appropriate level of secrecy. In this regard, there is a need to develop a systematic approach to simulate the process of data processing in the context of two streams: the control flow and the processing flow of critical data. The article proposes to model processes based on Petri nets in order to determine correspondence with the security policy approved in the organization in a hybrid cloud computing environment.

2. FEATURES OF OBJECTS WITH A STRUCTURALLY VARIABLE FORM OF CONTROL

2.1. Features of building a secure information environment based on cloud computing.

Public clouds are one of deployment models in which infrastructure and other computing resources are made available to the general public via the Internet. There is also a private cloud model where the computing environment works exclusively for the organization. Private clouds provide more control over infrastructure and computing resources than public clouds.

Two other common deployment models, which are the result of a combination of public and private clouds, are public and hybrid clouds. A public cloud has similarities with private clouds, but infrastructure and computing resources are common to several organizations that share a common level of confidentiality, security, and have common regulatory and legal aspects of management.

A hybrid cloud consists of two or more clouds (private, social or public), each of which has unique properties that are interconnected by a standardized or proprietary technology that provides general interaction.

Different deployment models affect the scope of activities and the number of controls over the cloud computing environment. In this connection, service models (delivery or deployment models) of cloud services [2] are generally distinguished: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

Figure 1 shows the differences in the actions and controls on the side of the cloud's client and the provider for each of the models presented. In the center of the diagram, five conceptual layers of the cloud environment which are characteristic both for public clouds and for other deployment models are distinguished [3].

Attitudes towards cloud services may vary significantly depending on:

- goals of the organization,
- structure of its assets,
- openness to the public,
- threats to which the organization is exposed,
- an acceptable level of information risk.

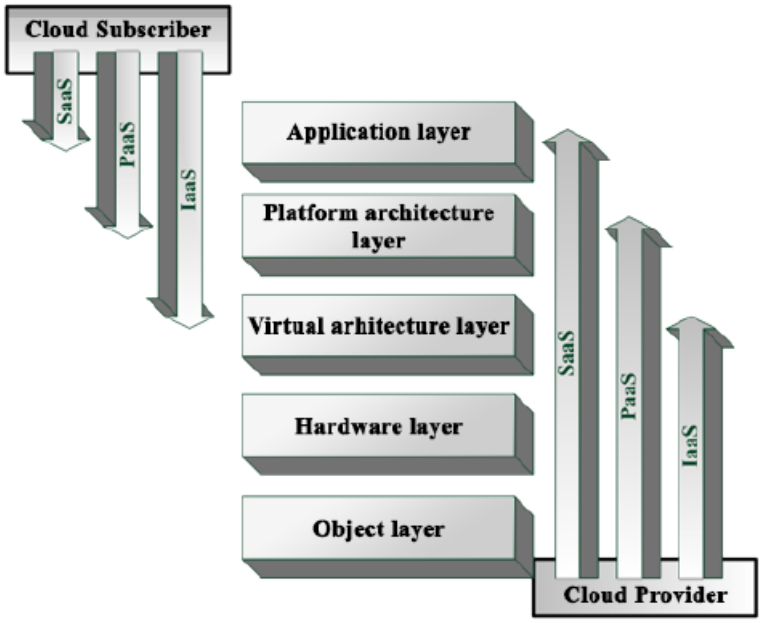

Figure 1. Scope of actions and controls between the client and the cloud provider within the conceptual cloud model

Information risk management, determining the suitability of cloud services for an organization is impossible without an understanding of the context in which an organization operates and the consequences of the possible types of threats it may face as a result of its activities.

Achieving the organization's information security objectives is key to making decisions about information technology outsourcing services and, in particular, to decide on the transfer of organizational resources to public clouds with the choice of provider and service agreement.

2.2. Model experiments on the migration of critical data to the hybrid cloud computing architecture

An organization's security policy is one or more rules, procedures, practices, or security guidelines that guide the organization in its activities [4]. Within the framework of security policy, we define the set of security subjects *S* and the set of objects *O*, the security function *f*, which for each object and subject determines the security level $l \in L$ as in a formula $f: S \cup O \rightarrow L$ [5].

While analyzing the Petri net, it is possible to obtain important information about the structure of a multi-level access control system in a hybrid cloud environment, which ultimately allows us to trace the dynamic behavior of the processing of critical data in the simulated system. This information is necessary for the following tasks:

1) estimation of the cost of building a hybrid architecture;

2) the choice of the optimal distribution of the processing of critical data between the public cloud environment and the private cloud environment;;

3) conducting a risk assessment and developing proposals for its improvement and change

Here are the key factors that confirm the effectiveness of using Petri nets to simulate data processing in a cloud computing environment [5]:

1) Petri nets were originally developed for modeling systems that contain interacting parallel components;

2) Petri nets allow us to describe the causal relationships between events;

3) actions of one component can be performed simultaneously with the actions of other components.

We will analyze the distribution of the critical data stream within the cloud computing environment based on the proposed calculations. Actions on the data will be displayed in the form of transitions of the Petri network in such a way that the task execution is connected with the implementation of the transition, as a result of which the network labeling appears, which determines the current state of the data processing process.

It is supposed to use data elements and their positions to determine two streams in the Petri net [5]: control flow and data stream.

In Figure 2, the data o_1, …, o_5 and the relationships between them (arrows) are depicted as a dashed line (data stream). The control flow is shown as a solid line (type data, ..., and their transitions).

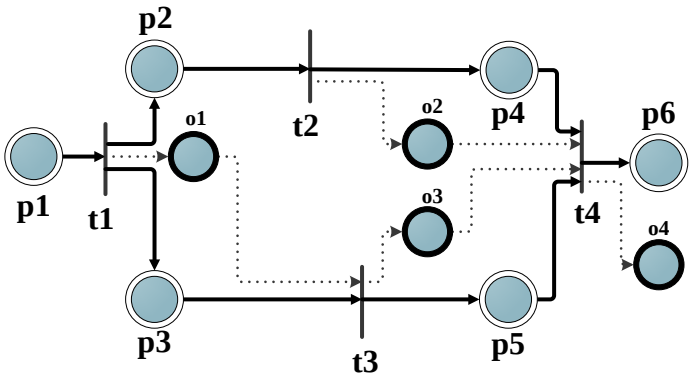

Figure 2. The processing of critical data depicted as a Petri net

Task execution requires the presence of a marker transmitted with data at the input position t and results in the creation of a marker at the output position t. That is, when executing the task t, the access to read data is determined by the presence of the input marker, the access to write data — the output marker. Figure 2 reflects the complete implementation of the data processing process, that is, the final state of the process is achievable.

Consider an example when a cloud service at the input receives data o_1 and o_3 and produces data o_4. The subject of the security policy must have access to read the data o_1 and o_3 and access to write data o_4. Then subject T must be able to read all the data with the marker and write data with the marker. The subject T and elements in the area $\bullet t \cup t \bullet$ are assigned the appropriate access levels in accordance with the requirements of the organization's security policy. The execution of the data processing should be controlled by a control element that creates various options for deploying the data processing. Determining whether a process is fully feasible, that is, the final marking is achievable from the starting marking, is a nontrivial task, but can be solved with the help of various analytics.

We define security subjects as $S=\{s_1,s_2,s_3\}$, data elements $O=\{o_1,o_2,o_3,o_4\}$, controls $P=\{p_1,p_2,p_3,p_4,p_5,p_6\}$, tasks / transitions $T==\{t_1,t_2,t_3,t_4\}$, for the initial position $M(p_1)=1$, other markings for it are equal to 0. Figure 3 shows 6 states of data processing in the form of nodes. Each state is characterized by two columns: the first of the columns (p) represents the state of the control flow, the second (o) the state of the data flow. For example, node V has markers for data $\{p_4,p_5\}$ (column to the left of node V), $\{o_2,o_3\}$ (right column of node V).

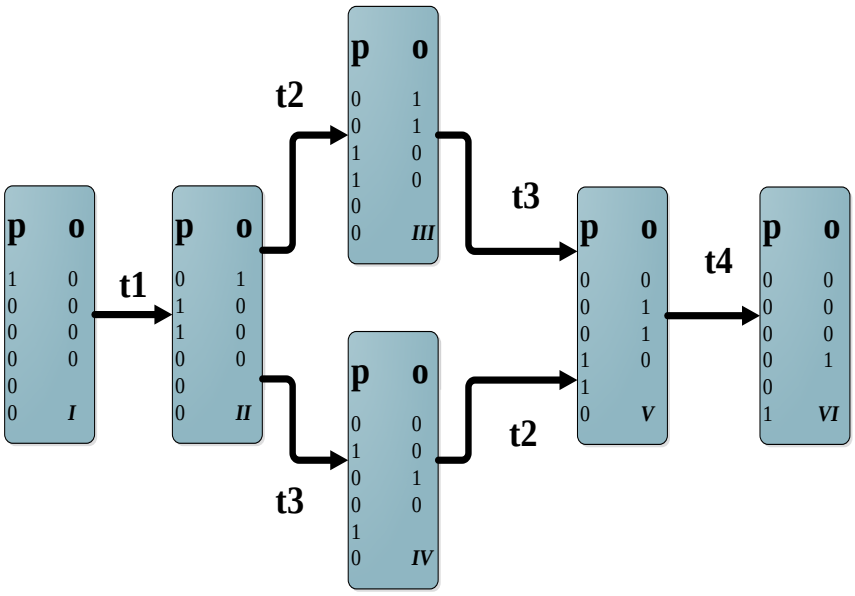

Figure 3. Data Processing States

We take into account the requirements of the security policy "*" and "ss" of the classical access model Bella LaPadula [6]. For clarity of the example, we will define a scale of information security levels consisting of two levels: “Secret” and “Unclassified”. We assign security levels for the subjects of the process in question, so that all tasks will inherit the authority of the role under which they are performed (Table 1).

Table 1. Cloud Service Access Levels

Security function	**Information Security Level**
$f(t_1)= f(t_2)= f(t_4)$	low (unclassified)
$f(t_3)$	high (top secret)

The principles of building a Petri net according to safety requirements will be presented in the form of the following positions [7].

If the subject (cloud service) has a high level of access, then:

– it is allowed to make the transition from node N to node M, as a result of which data is recorded with a high level of secrecy;

– it is allowed to make the transition from node N to node M, as a result of which data of high or low levels of secrecy is read;

– it is forbidden to make the transition from the node N to the node M, as a result of which the data of low level of secrecy are recorded.

If the subject (cloud service) has a low level of security, then:

– it is allowed to make the transition from node N to node M, as a result of which data is recorded with a high or low level of secrecy;

– it is allowed to make the transition from node N to node M, as a result of which data of a low level of secrecy are read;

– it is forbidden to make the transition from node N to node M, as a result of which data of a high level of secrecy is read.

As a result of applying these principles, a graph is formed that takes into account the assigned access levels of all subjects of the process under consideration and, depending on the authorities, a decision is made on data labeling (Figure 4). Figure 4 consists of 15 nodes, which show the possible markings of the processed data in the Petri net. The values p_1,p_2,p_3,p_4,p_5,p_6 of the first column show the marking of the control flow, the values o_1,o_2,o_3,o_4 of the second indicate the marking of the data flow with the appropriate levels of security (confidentiality) for. For example, node XI has two data control labels p_2, p_3, a high security data label o_3, and a low security data label o_2.

For clarity and better perception of the Petri net, it is proposed to use different colors for each node.

1. Nodes, within which the processing of critical data takes place, are colored red and correspond to the component of the private cloud computing environment.

2. Nodes within which the processing of unclassified data takes place are colored green. These nodes can be deployed in a public cloud computing environment that has a lower cost than a private one.

The constructed Petri net has two types of control arrows:

1) the solid line is used to describe the valid marking, where there are no violations of the requirement "*" and "ss";

2) the dotted line describes the labeling of data that violates one of the requirements of the security policy.

3. DISCUSSION AND RESULTS

Selectively, we give examples of violation of the security policy of a constructed graph (the presence of a dotted line) in Figure 4.

- ✓ The transition from state II to state VI violates the "ss" requirement, that is, it is prohibited to make the transition from node N to node M, as a result of which the subject with a high level of security (t_3) initiates the recording of low-level secrecy data (o_3).
- ✓ The transition from state XII to state XV violates the "*" requirement, that is, the prohibition of reading information with a high level of secrecy o_2,o_3 by a subject with a lower level of security (t_4).

If a three-level privacy scale is introduced into the model, it is possible that a subject with an average level of security will request read access to data with a high level and initiate the recording of an object with a low level of secrecy. These actions will violate both requirements of the security policy built on the requirements of Bella LaPadula.

If a three-level privacy scale is introduced into the model, it is possible that a subject with an average level of security will request read access to data with a high level and initiate the recording of an object with a low level of secrecy. These actions will violate both requirements of the security policy built on the requirements of Bella LaPadula.

A detailed analysis of Figure 4 shows that there is no route that fully satisfies the safety requirements and makes it possible to transition from state I to state XIV or XV. For this example, the requirements of "ss" and "*" turned out to be impossible.

You can consider different solutions to the problem.

1.Adapt the current Petri net and incorporate new elements into it. Introduction to the model of demilitarized zones, the role of which private clouds can perform, will make it possible to build a route, the fulfillment of which will fulfill the basic requirement of accessibility to the Petri nets. A private cloud should be deployed to handle states in which, as a result of transitions (task execution), critical data are created (with a high level of secrecy).

2.Change, if possible, the security grid for cloud services and data with a subsequent change in security policy, for example (Table 2).

3.

Table 2. Security grid

Security function	**Information Security Level**
$f(o_1)= f(o_3)= f(o_4)=f(o_5)$	High
$f(o_2)$	Low

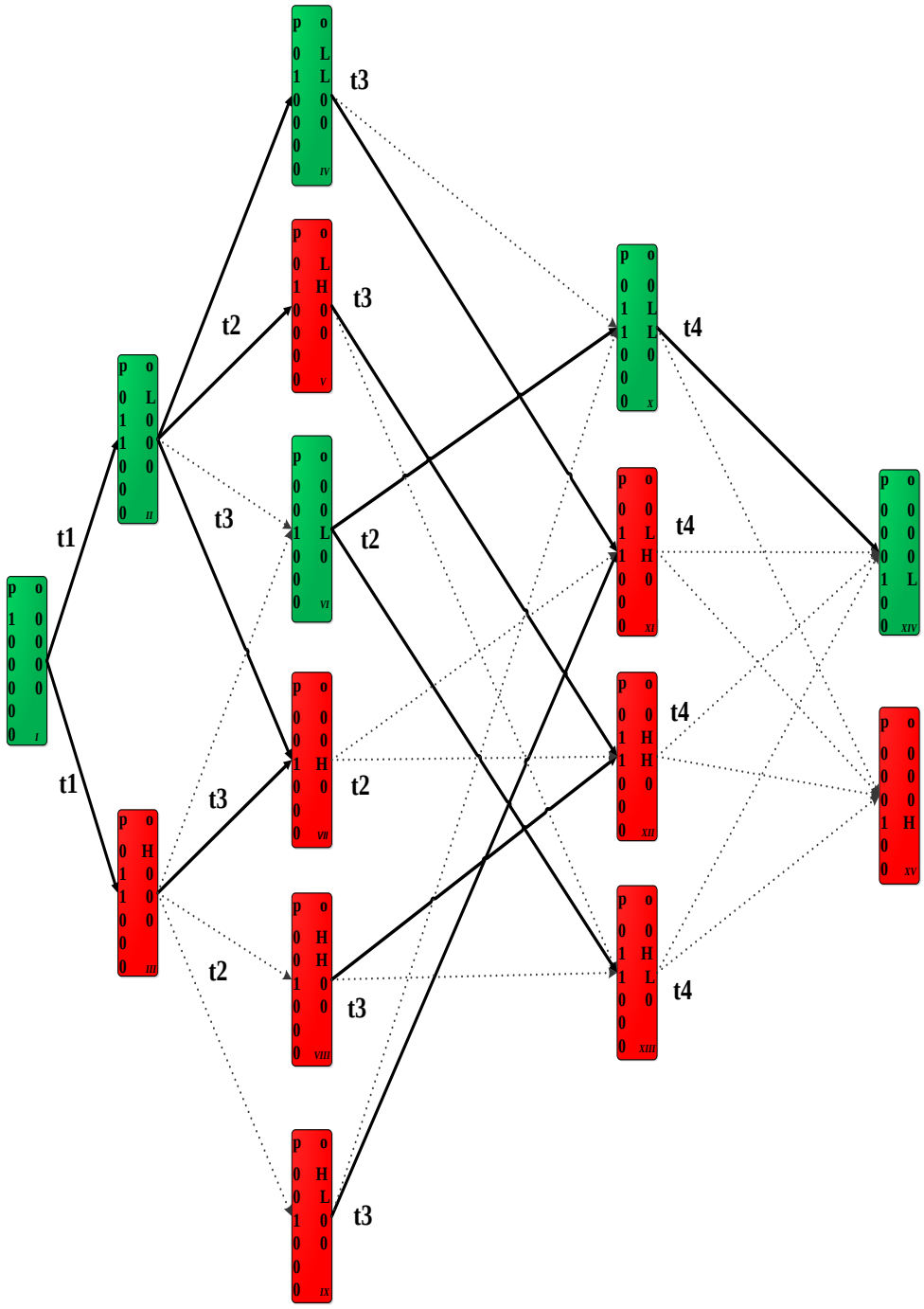

Figure 4. Petri net with assigned levels of privacy for data and service

The proposed method allows for a formal analysis of a multi-level security model for the information flow of a business process as a function of time. The use of the state graph obtained on the basis of the Petri net allows to improve and dynamically change the processing of critical data depending on current conditions.

The described approach is proposed as the basis for automating the separation of workflows within a hybrid cloud computing environment. This approach should replace the process of selection by the administrator of a possible distribution of processes, which is subjective and may lead to an error. Replacing the manual definition is proposed to introduce an automatic mechanism that implements the work of the described method, which will determine the permissible parameters based on a strict set of rules, and then suggest the best one based on the value model. The considered approach has advantages that can reduce both potential security breaches and reduce the cost of IT infrastructure.

4. CONCLUSION

The proposed approach to modeling the processing of data using Petri nets based on the requirements of an organization's security policy provides important information about the structure of a multi-level access control system in a hybrid cloud environment, which ultimately allows tracing the dynamic behavior of critical data processing in the simulated system. This information will be useful for the following tasks.

1.Estimating the cost of building components of a hybrid cloud computing environment.

2.The choice of the optimal distribution of the processing of critical data between the public and private cloud.

3.Conduct a risk assessment for each component and develop proposals for the improvement and modification of the selected architecture.

When considering more complex cases, if the weights of violations and their possible consequences (increase in security levels, number of positions and subjects in the network) are known in advance, it is recommended to search for the minimum (optimal) route using the constructed graph.

REFERENCES

[1] Suicimezov, N., Georgescu, M. IT governance in Cloud. *Procedia Economics and Finance*, vol. 15, 2014, pp. 830-835.

[2] Mell, P., Grance, T., The NIST Definition of Cloud Computing, *Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145, 2011, p. 6.

[3] Tsaregorodtsev, A.V., Kachko, A.K. One of the approaches to the management of information security in the development of information infrastructure of organization. *National Security*, 1 (vol. 18), 2012, pp. 46-59.

[4] Tsaregorodtsev, A.V., Kislytsin, A.S. *Basic principles of protected telecommunication systems syntheses*. Moscow: Radiotechnika, 2006, pp. 243-254.

[5] Mayr, Ernst W. An Algorithm for the General Petri Net Reachability Problem. *SIAM Journal*, 3 (vol. 13), 1984, pp. 441-460.

[6] Bell, D.E., LaPadula, L.J. Secure *Computer System: Unified Exposition and Multics Interpretation*, Tech report ESD-TR-75-306, Massachusetts, Bedford: The Mitre Corporation, 1976, 134 p.

[7] Tsaregorodtsev, A.V., Kravets, O.Ja., Choporov, O.N., Zelenina, A.N. Information Security Risk Estimation for Cloud Infrastructure. *International Journal on Information Technologies and Security*, 4 (vol. 10), 2018, pp. 67-77.

[8] Vasilyev, V.V., Shamsutdinov, R.R. Intelligent system of information security incident analysis (based on the methodology of SIEM-systems using immunocomputing mechanisms). *Modeling, optimization and information technologies*. 1 (7), 2019, pp. 536-547.

[9] Vorobyev, E.I., Preobrazhenski, Y. P. The investigation of error-correcting coding of the variousfiles. *Modeling, optimization and information technologies*, 4 (6), 2018, pp. 535-544.

[10] Lapina, T.I., Dimov, E.M., Petrik, E.A., Lapin, D.V. Access controls to information resources in information systems. *Modeling, optimization and information technologies*, 4 (6), 2018, pp. 523-534.

Information about the authors:

Anatoly Valerjevich Tsaregorodtsev – doctor of Sciences (Engineering), Professor, Dean of International Information Security Faculty, Head of Information Security Department,

Igor Yakovlevich Lvovich – doctor of Sciences (Engineering), Professor, Rector at Voronezh institute of high technologies,

Marat Siradzheddinovich Shikhaliev – postgraduate student, Russian university of transport,

Anna Nikolaevna Zelenina – candidate of Technical Sciences, Associate Professor, leading specialist of the project department at Voronezh institute of high technologies,

Oleg Nikolaevich Choporov – doctor of Sciences (Engineering), professor at Voronezh state technical university, areas of scientific research – system analysis, optimization, simulation of complex objects.

Manuscript received on 08 June 2019