Functional Organization and Evaluation of Access Management System with Heterogeneous Resources

RADI ROMANSKY & IRINA NONINSKA

Contents

Abstract

The contemporary Information Society is based on different digital technologies which are very useful in improving process efficiency, but can also have a negative impact on personal privacy.

The purpose of this article is to present an organization of processes in a business system for access managing to different types of resources – public type and protected type which are determined as internal (in own storages) and external (located in a cloud). It is accepted that some of resources contain personal data (profiles of staff, users, etc.), which necessitates discussing potential privacy and data protection issues.

Formalization of communications in e-space and functional description of processes in the proposed management system are presented. An evaluation of procedures correctness by using stochastic modelling is made.

I. Introduction

Many information resources are accessed remotely via global network which required a strong regulation based on strategy of management. These resources could be two types: public (without any restriction to use) and private (protected information located in different distributed in global network nodes, including in the cloud). The second type requires special measures for data protection and access regulation.

The regulation of the access to the resources and using is a task of special management system which must be developed on the base of strong policy for information security and data protection. The design of such system should be preceded by preliminary formalization and additional organizational processes (suitable modelling and functional algorithm).

An organization and investigation of Access Management System is the object of this article.

II. Related Works

Review of some publications in the field of the discussed problem is made in this section. It is stated that many applications in the business and administrative organizations use cloud services for support own information resources, including personal profiles of users and staff. This creates a possibility for cross-boarder data transfer, which can violate some GDPR requirements.

Very important part of the access control is to select or define adequate policy model and suitable framework – a new context-aware access control is proposed in reviewed publications, which is based on determined formal policy model and policy ontology for modelling. The authors extend this model in case of cloud-based data.

Another reviewed article discusses the theme of information security whit formulating some recommendation for research.

The rest references are related to the role-based access control, cloud data protection, security requirements, etc.

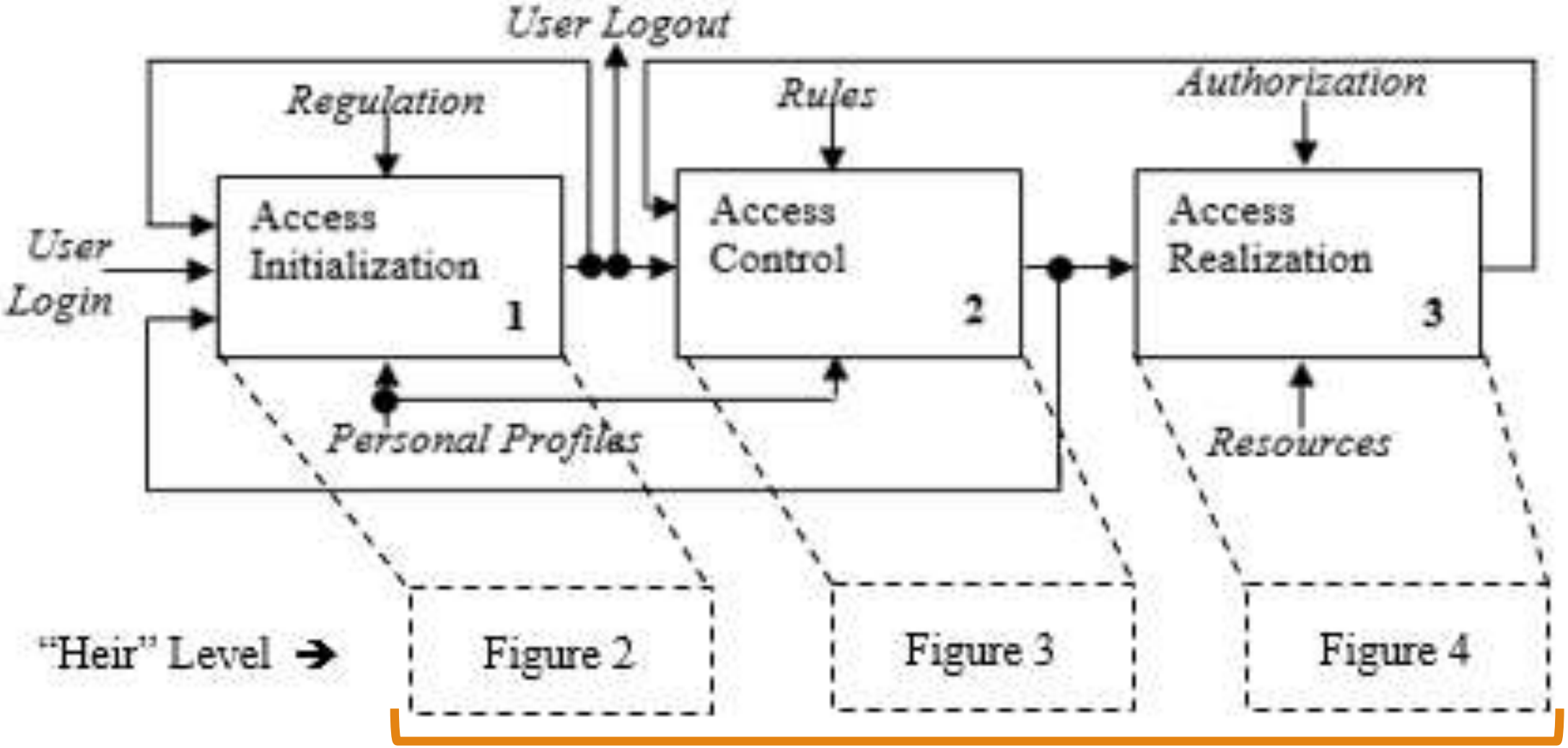
III. Functional Organization of Process in Access Management System (AMS)

Functionality and structural organization of an AMS are determined by realization of preliminary modeling using IDEF0 standard, part of technology for modelling and conceptual design IDEF (Integrated DEFinition).

This technology was developed in the frame of the US program Integrated Computer-Aided Manufacturing as a collection of standards and IDEF0 is a basic standard for functional modelling of processes in a system by representing them as a set of interdependent actions or functions.

The IDEF0 model has a "parent / heir" hierarchical structure obtained by functional decomposition of the underlying process of the sub-processes. The main organization of the model in the “parent” level is shown in the next figure.

Functional IDEF0 model of AMS organization – "parent" level



Presented in the next slide

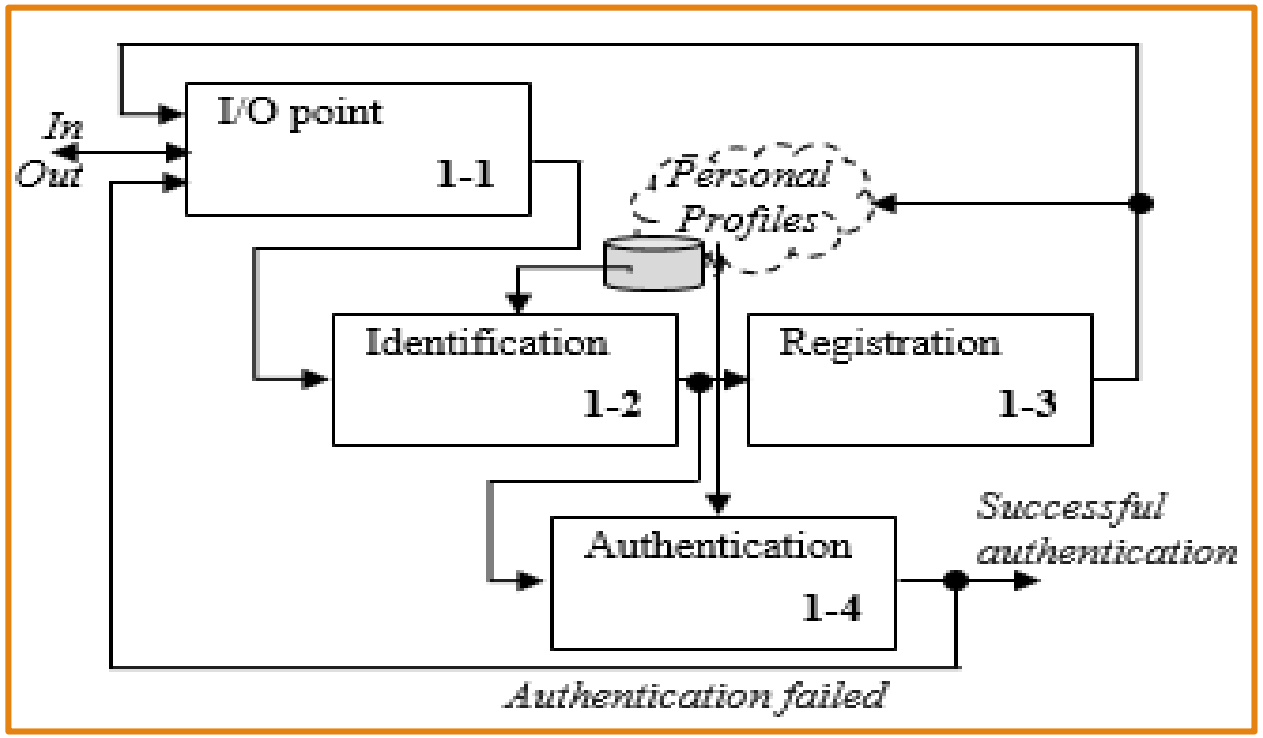


Figure 2

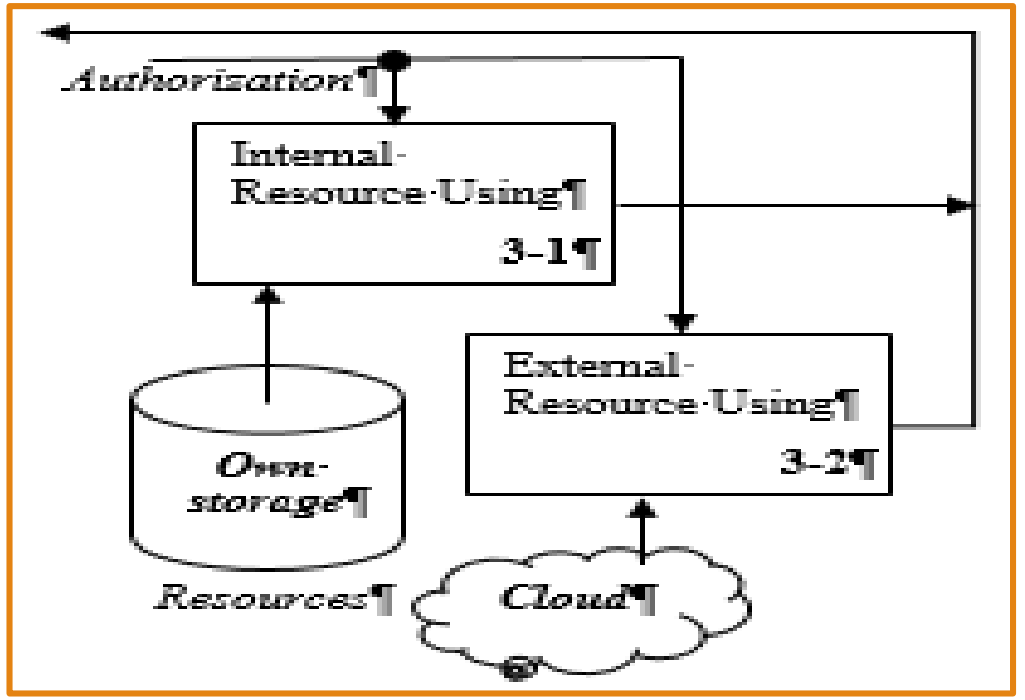


Figure 4

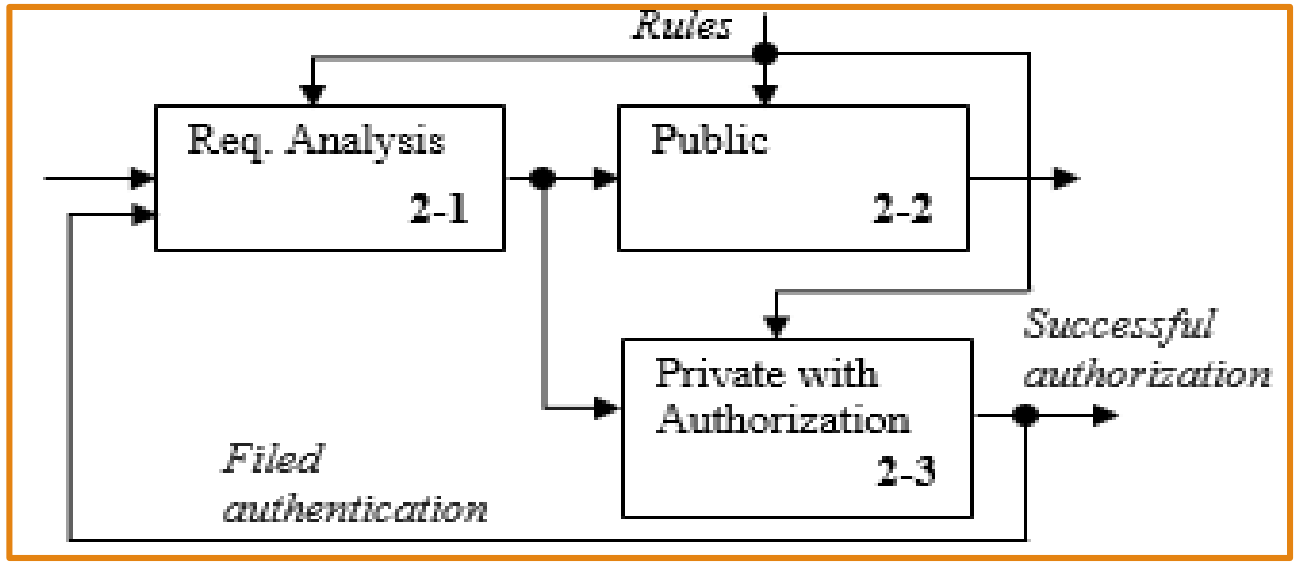


Figure 3

Algorithmic description of the AMS Functionality

Start a process

Procedures realised by the Front-office sus-system

Procedures realised by the Back-office sus-system

Access and using protected resources

Exit from the AMS

```
[1]  begin
[2]     IF  user access = YES      THEN  [3]      ELSE  [2]
[3]        <Service process activation>
[4]        <Procedure "Identification">
[5]     IF  identification = OK      THEN  [8]
[6]        <Procedure "Registration">
[7]     go to [3]
[8]        <Procedure "Authentication">
[9]     IF  authentication ≠ OK      THEN  [24]
[10]       <Procedure "Request Analysis">
[11]    IF request_type = FINISH      THEN [24]]
[12]    IF request_type = PRIVATE      THEN [15]
[13]       <Public resource using>
[14]    go to [10]
[15]    input in private system
[16]          <Procedure "Authorization">
[17]       IF  authorization ≠ OK     THEN [10]
[18]          <Authorized access analysis>
[19]             IF  access = CLOUD      THEN [22]
[20]                <Internal protected resource using>
[21]             go to [10]
[22]                <External/cloud protected resource using>
[23]             go to [10]
[24]    out of system
[25]  end
```

IV. Evaluation of the Processes in AMS

A stochastic model by using the apparatus of Markov's random processes is developed to study the AMS behavior and to evaluate the correctness of supported procedures and processes. The definition is follows:

TABLE 1. STATES DEFINITION OF THE MARKOVIAN MODEL

[j]	S_j	Description of the state
[1]	S_1	Initial point for communication with users (input/output state)
[4]	S_2	Procedure for preliminary identification (ID) of a user's access to the system
[6]	S_3	Procedure for initial registration of a new user which is requested a service/activity
[8]	S_4	Procedure for authentication of registered user successfully passed ID
[10]	S_5	Procedure for analysis of current request for access and use system information resource
[13]	S_6	Allowed access and use of not protected public resource (access without restriction)
[15] [16]	S_7	Input in the protected private part of the system with procedure for authorization activation
[20]	S_8	Allowed access and use of internal information resource stored in own storages
[22]	S_9	Allowed access and use of external information resource stored in cloud

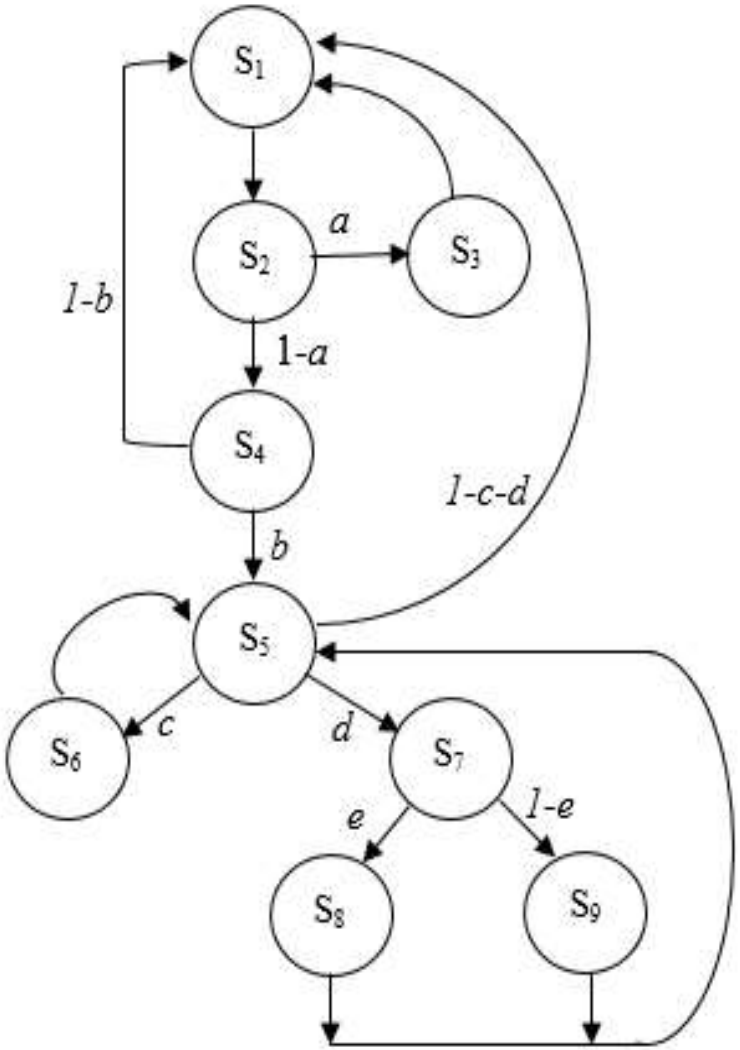
Vector of initial probabilities

$P_0 = (1, 0, 0, 0, 0, 0, 0, 0, 0)$.

TABLE 2. TRANSITION MATRIX DEFINITION

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9
S_1	0	1	0	0	0	0	0	0	0
S_2	0	0	a	$1-a$	0	0	0	0	0
S_3	1	0	0	0	0	0	0	0	0
S_4	$1-b$	0	0	0	b	0	0	0	0
S_5	$1-c-d$	0	0	0	0	c	d	0	0
S_6	0	0	0	0	1	0	0	0	0
S_7	0	0	0	0	0	0	0	e	$1-e$
S_8	0	0	0	0	1	0	0	0	0
S_9	0	0	0	0	1	0	0	0	0

Graph of the states of the defined model



Analytical definition of the Markovian model for evaluation of supported in AMS processes

$$
\begin{array}{|l|l}
1 & p_1 = ap_3 + (1-b)p_4 + (1-c-d)p_5 \\
2 & p_2 = p_1 \\
3 & p_3 = ap_2 \\
4 & p_4 = (1-a)p_2 \\
5 & p_5 = b.p_4 + p_6 + p_8 + p_9 \\
6 & p_6 = cp_5 \\
7 & p_7 = dp_5 \\
8 & p_8 = ep_7 \\
9 & p_9 = (1-e)p_7 \\
10 & \sum_{j=1}^{9} p_j = 1
\end{array}
$$

Analytical solution of the model:

(a) presentation

$p_2 = p_1;$ $p_3 = ap_1;$ $p_4 = (1-a)p_1;$ $p_5 = \frac{(1-a)b}{(1-c-d)}p_1;$ $p_6 = \frac{(1-a)bc}{(1-c-d)}p_1;$

$p_7 = \frac{(1-a)bd}{(1-c-d)}p_1;$ $p_8 = \frac{(1-a)bde}{(1-c-d)}p_1;$ $p_9 = \frac{(1-a)(1-e)bd}{(1-c-d)}p_1$

(b) solving the last equation [10]

$p_1 \frac{3(1-c-d)+(1-a)(b+bc+2bd)}{(1-c-d)} = 1$ ➔ $p_1 = \frac{x}{3x+(1-a)(b+bc+2bd)}$; **at *x* = (1-*c*-*d*)**

(c) final analytical presentation of the probabilities

$3.x + (1-a).(b + b.c + 2b.d = y$

$$p_1 = p_2 = \frac{x}{y};\quad p_3 = \frac{a.x}{y};\quad p_4 = \frac{(1-a)x}{y};\quad p_5 = \frac{b(1-a)}{y}$$

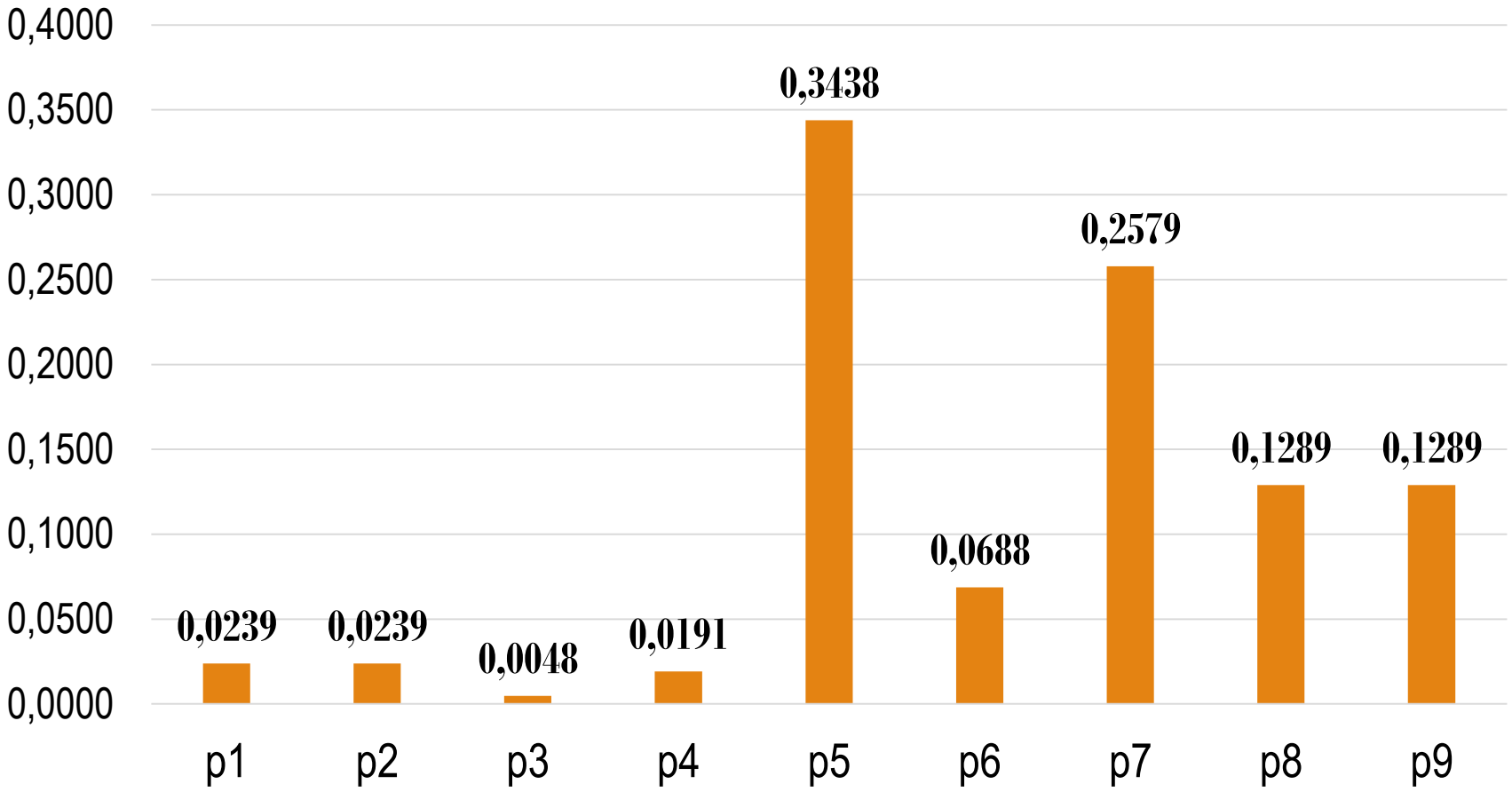
$$p_6 = \frac{bc(1-a)}{y};\quad p_7 = \frac{bd(1-a)}{y};\quad p_8 = \frac{bde(1-a)}{y};$$

$$p_9 = \frac{bd(1-a)(1-e)}{y}$$

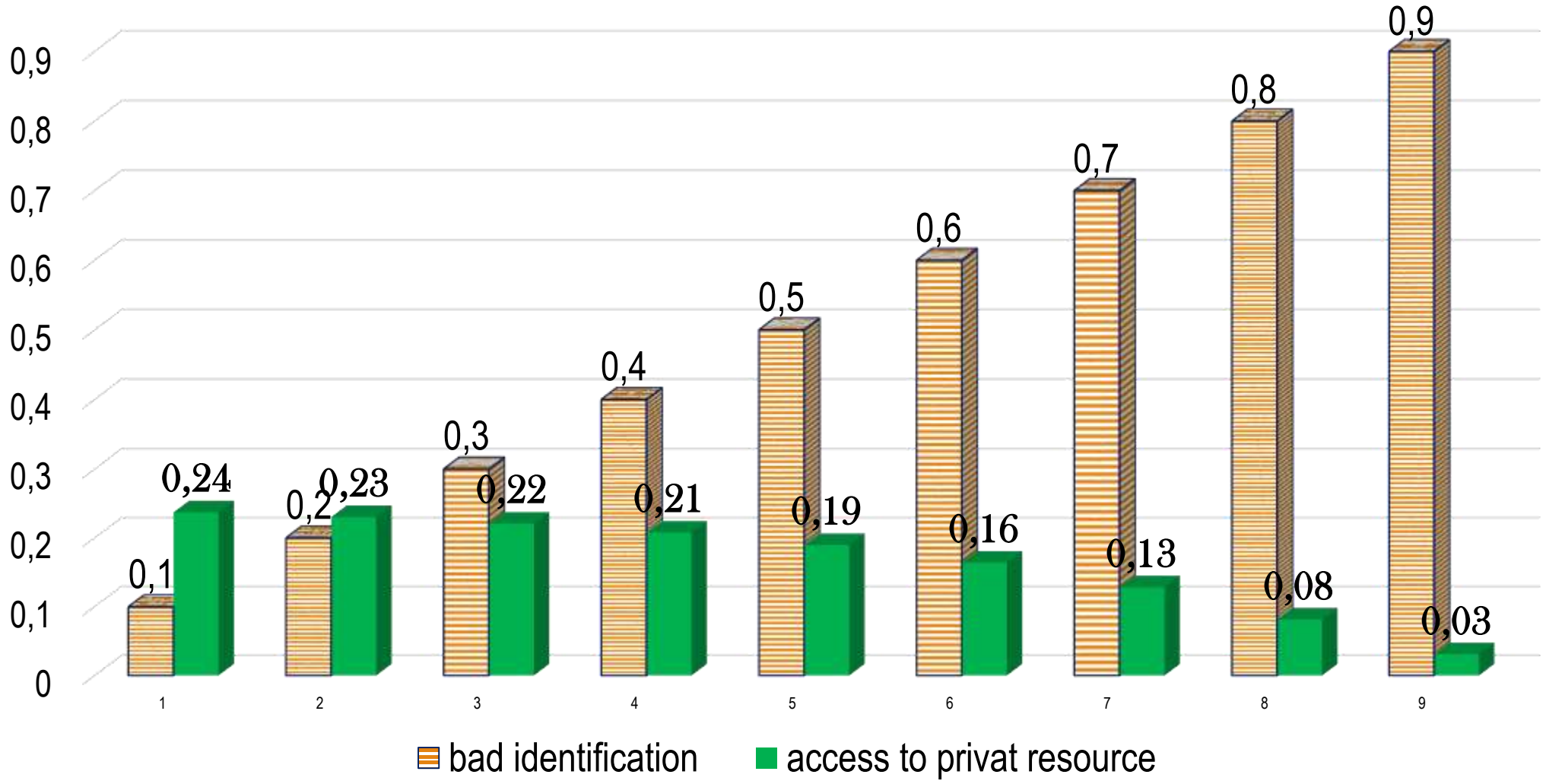
(d) some experimental results

A partial factorial plan based on fixed values for {*a*, *b*} and selected conditions' values for {*c*, *d*, *e*} has been adopted, because the main goal is to evaluate correctness of procedures for secure access in case of correct user's request (successful identification and authentication).

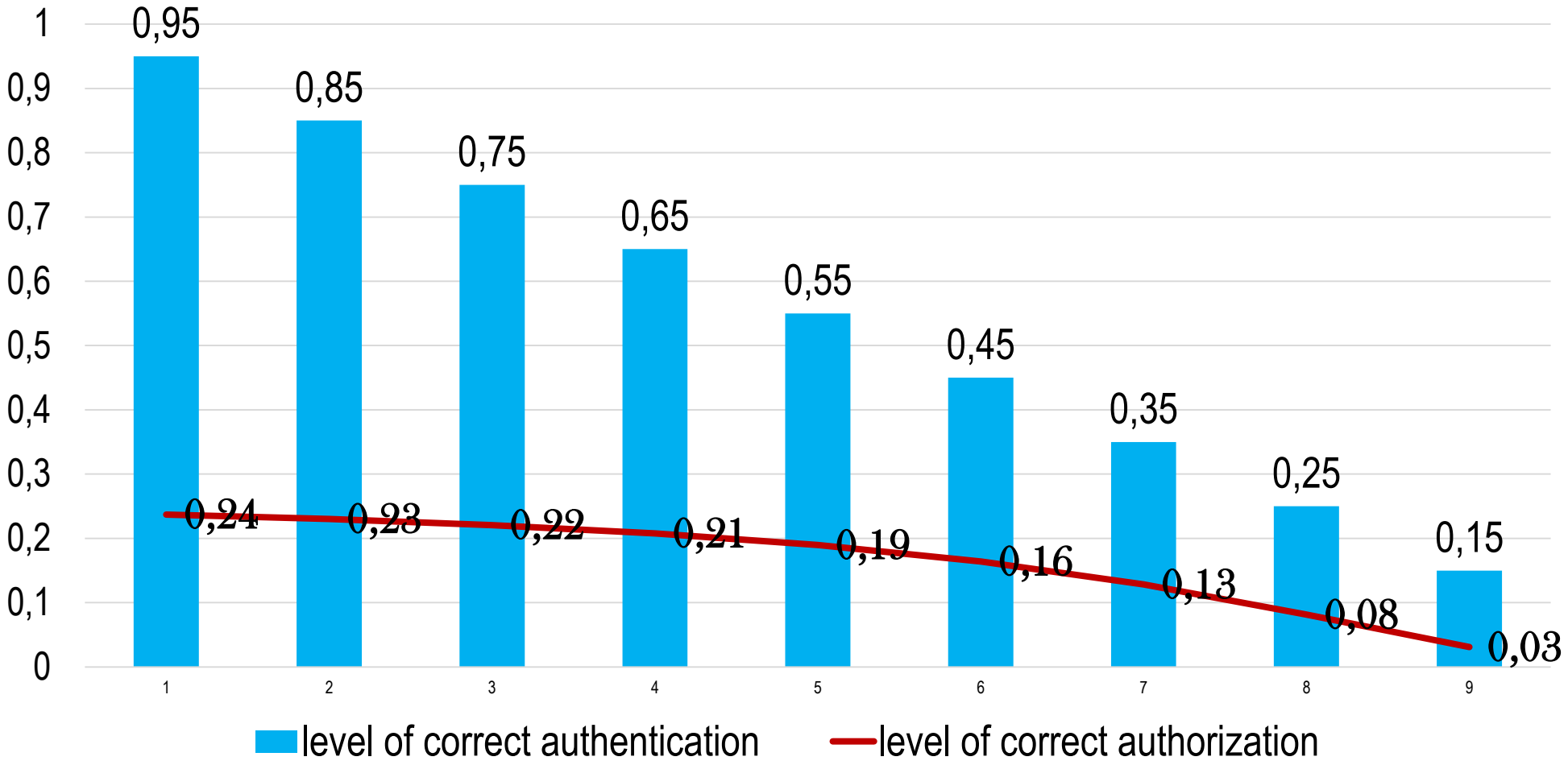
Distribution of the state probabilities for a typical situation



*Relation between level of **incorrect identification** and probability of **entering the protected sub-system***



*Evaluation of the relationship between the probabilities of **successful authentication and authorization***



V. Conclusion

The mine requirements for protection of distributed information resources in the cyber space can be summarized as a protection of the integrity (from unauthorized deletion, modification, theft) and the availability (access to services, data and resources anywhere and anytime). Each AMS must ensure that the procedures for regulated access to remote resources are properly implemented. For this purpose, it is necessary to implement the principles of the "CIA triad" (confidentiality, integrity, availability), developed information security policy and specific requirements for data protection, including personal data and profiles.

References

[1] Giorgio Audrito, Sergio Bergamini, "Effective collective summarization of distributed data in mobile-agent systems", Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems - AAMAS'19, Montreal, Canada, May 2019, pp. 1618-1626.

[2] Han Qui, Hassan Noura, Meikang Qui, Zhong Ming, and Gerard Memmi, "A user-centric data protection method for cloud storage based on invertible DWT", IEEE Transactions on Cloud computing, April 2019,

[3] Nicolas Mundbrod, Manfred Reichert, "Object-specific role-based access control", International Journal of Cooperative Information Systems, vol. 28, no. 1, 2019, pp. 1950003-1 – 1950003-30

[4] A. S. M. Kayes, Jun Han, "Context-aware access control with imprecise context characterization for cloud-based data", Future Generation computer Systems, vol. 93, April 2019, pp. 237-255

[5] A. S. M. Kayes, Jun Han, W. Rahayu, T. Dillon, M. S Islam, A. Colman, "A policy model and framework for context-aware access control to information resources", The Computer Journal, vol. 65, no. 5, May 2019, pp. 670-705

[6] Joanna Paliszkiewicz, "Information security policy compliance: Leadership and trust", Journal of Computer Information Systems, vol. 59, no. 3, 2019, pp. 211-217

[7] Romansky, R., Irina Noninska, "Discrete formalization and investigation of secure access to corporative resources. International Journal of Engineering Research and Management, vol.3, no. 5, May 2016, pp. 97-101.

[8] A. B. Cheryshov, O, N. Choporov, A. P. Preobrazhenskiy, O. Ja. Kravets, "The development of optimization model and algorithm for support of resources management in organizational system", International Journal on IT and Security, vol. 12, no. 2, Jun 2020, pp. 25-36.

[9] Ang Cheng-Leong, Khoo Li Pheng and Gay Robert Keng Leng, "IDEF*: A comprehensive modelling methodology for the development of manufacturing enterprise systems", International Journal of Product Research, vol. 37, no. 19, 1999, pp. 3839-3859.

[10] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, "Anonymous and traceable group data sharing in cloud computing", IEEE Transactions on Information Forensics and Security, vol. 13 No. 4, 2018, pp. 912-925.

Thank you for your attention

Radi Romansky

rrom@tu-sofia.bg

Irina Noninska

irno@tu-sofia.bg