ISSN 1992-6502 (Print)
Vol. 17, no. 6 (59), pp. 3-12, 2013.
Vestnik UGATU
ISSN 2225-2789 (Online)
http://journal.ugatu.ac.ru

UDC 004.7

# COGNITIVE MAPS FOR RISK ASSESSMENT IN PROVIDING CLOUD COMPUTING DATA SECURITY

U. KONRAD[1], V. J. PENZINA[2]

[1] u.konrad@hzdr.de, [2] penzina.vladislava@gmail.com

[1] Helmholtz Zentrum Dresden-Rossendorf, Germany
[2] Ufa State Aviation Technical University (UGATU), Russian Federation

*Submitted 2013, June 10*

**Abstract.** Cloud Computing (CC) became a new milestone in era of information technology. Almost unlimited possibilities for the storing information, data processing and virtual machine creation discovered unique perspectives. However, new technologies bring new threats, risks and serious consequences.

**Keywords:** cognitive maps; risk assessment; cloud computing; data security

## 1. INTRODUCTION

Cloud computing is based on distributed computing, parallel processing, virtualization and grid computing and is the commercial implementation of the concepts above. Since Eric Schmidt, the CEO of Google, first openly used the concept of "cloud computing", cloud computing have swept the Internet and triggered a global research and development boom. International large companies such as Amazon, Google, IBM, Microsoft and Yahoo are pioneers in CC. Many other companies like Salesforce, Facebook, Youtube, Myspace also make a success in cloud computing. [1]

Cost contraction with respect to investment, reduction of development and information services costs, decrease of administrative functions and rise of business flexibility – obvious advantages of cloud technologies that enable companies to meet the needs of a rapidly changing market environment. [2]

This article gives the definition of cloud computing, its basic models, services and security issues. It also displays a list of main threats, and proposes a solution for their identification using fuzzy cognitive maps. Further presented an example of introduced approach embodied in MATLAB. Article ends with conclusions and plans for future research.

## 2. CLOUD COMPUTING

Since the cloud computing specification of National Institute of Standards and Technology (NIST) has been proposed, the definition of NIST about cloud computing becomes the most authoritative one widely accepted by researchers: CC is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [3]

The cloud computing definition of NIST includes five essential features, three service models and four deployment models as figure 1 shown.

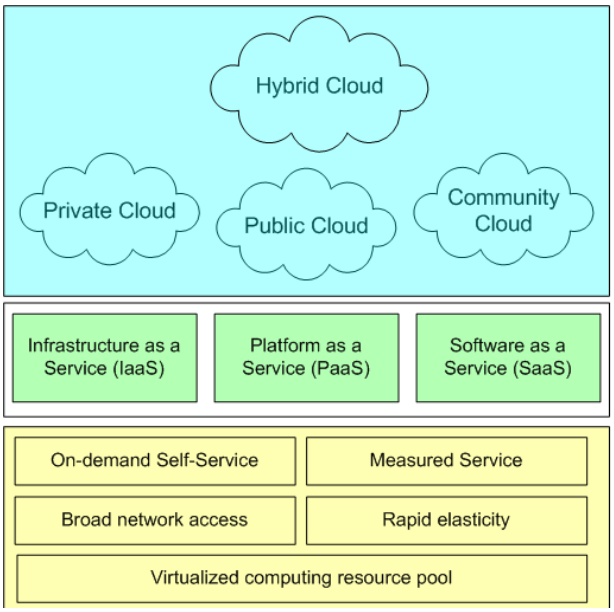


**Fig. 1.** Cloud Computing NIST definition

The dividing line between the three layers of service models is not clear and, in fact, there is a considerable amount of overlap. For example, a software system may be considered as part of a software platform; similarly, an IS platform may be considered as part of IS infrastructure. It is for this

reason that researchers have also discussed combined models such as: SaaS & PaaS; SaaS & IaaS; IaaS & PaaS; and even SaaS &PaaS & IaaS. Numerous other categories have also been suggested in recent years e. g.:

- Storage-as-a-Service;
- Database-as-a-Service;
- Security-as-a-Service;
- Communication-as-a-Service;
- Management/Governance-as-a-Service;
- Integration-as-a-Service;
- Testing-as-a-Service;
- Business Process-as-a service.

Cloud computing is introducing huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always in focus, and a big barrier for its widespread applications.

## 3. CLOUD COMPUTING SECURITY ISSUES

Security – first fear during the transition to the cloud. Users need to be assured that their data will be stored safely. Provision of confidentiality, integrity and availability of information is a key factor in the cloud services trust use. Examples of the "cloud" catastrophes show that thoughtless attitude to safety issues have serious consequences: accident on the Amazon Web Service in 2011, permanently destroyed data of various clients, hacking Sony Playstation Network in April 2011 revealed access to 10 million credit cards [4, 5].

According to CSA "Top Threats to Cloud Computing", there are 7 main threats affecting CC services [6]:

1. Abuse and nefarious use of cloud computing – by abusing the relative anonymity behind registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity;

2. Insecure interfaces and APIs – the security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy;

3. Malicious insiders – this threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure;

4. Shared technology issues – IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e. g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources;

5. Data loss or leakage – the threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment;

6. Account or service hijacking – cloud solutions add a new threat to the landscape. If an attacker gains access to users credentials, they can eavesdrop on user activities and transactions, manipulate data, return falsified information, and redirect them to illegitimate sites;

7. Unknown risk profile – versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs.

Other sources are also assigning: personal data duplication, confidentiality of the personal data, cloud environment breach isolation, cloud infrastructure security, inadequate security testing environments, privileged access to data, compliance, data location, isolation data, data recovery, incident investigation, long-term data availability [7].

In this paper we will concentrate on threats that most likely will affect user (end-users or company, which is providing services), in Private cloud and PaaS and SaaS service models.

## 4. CC SECURITY CONCEPTUAL, FUNCTIONAL AND MATHEMATICAL MODELS

In order to define appropriate set of threats, that will influence users' cloud services, it is necessary to identify their (threats') sources. Conceptual models of possible scenarios usage of CC services are represented on fig. 2.

Subject to different scenarios (e.g. Fig.2 a, b, c), various sets of threats will take place. Since considering only SaaS and PaaS, most of the responsibility lie on service providers, thereby our task is to assure internal protection, data security (inventory, encryption) and meticulous verification of all Service Level Agreements (SLA) paragraphs.

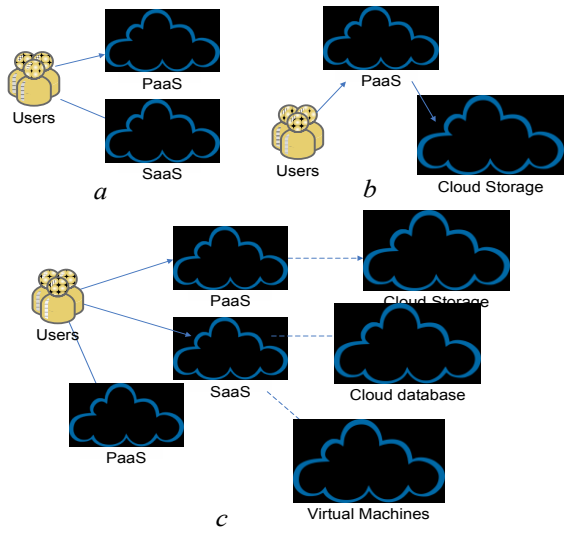


**Fig. 2.** CC service usage scenarios

For example, for European countries it can become critical factor of where data, which will be processed at PaaS level, will be stored (Fig. 2, *c*). The Safe Harbor framework and USA Patriot Act create new challenges and subtleties according to legal regulations between United States of America and European Union. Risk of information disclosure according to Washington official request, as long as both sides (USA and EU) will not come to unified verdict, still exists [4, 8].

Despite the limitations, a variety of CC risks require a system that can stipulate the probability of threat, assess risk level and offer recommendations for reducing it. For a more detailed examination of CC risk assessment issue, a functional model using a methodology of structural analysis and modeling SADT was developed (Fig. 3).

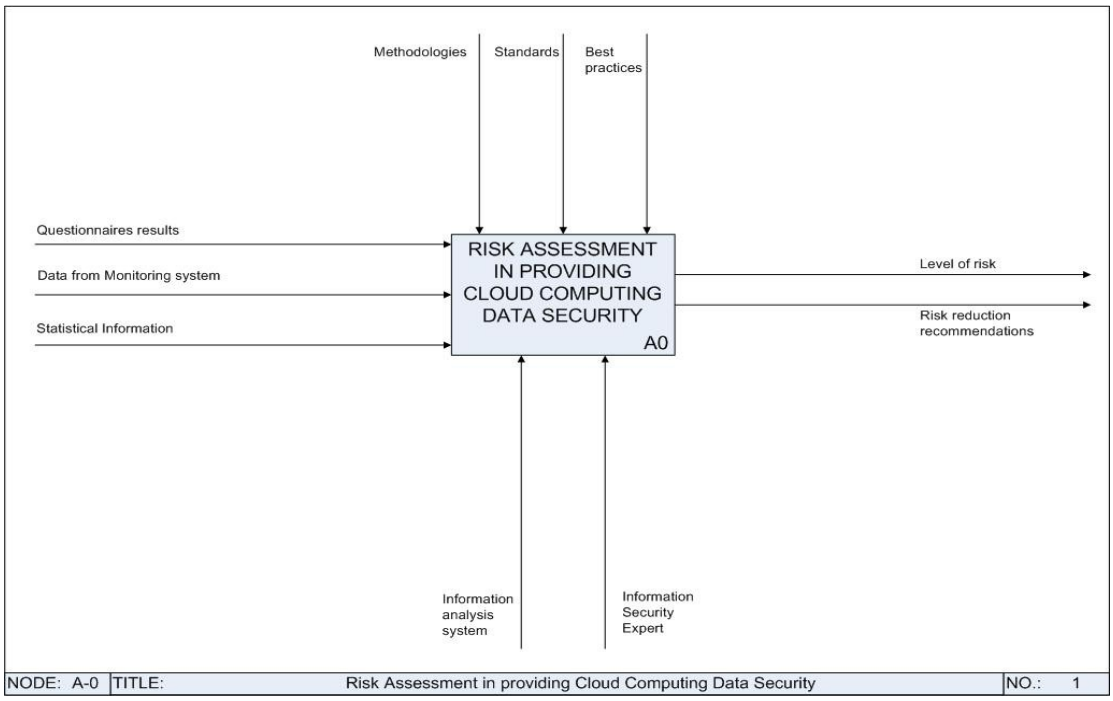


**Fig. 3.** Context diagram of CC risk assessment process

Input data consist of statistical information, data from monitoring systems (Network-layer, application-layer, local operating system-layer vulnerability scans monitoring) and questionnaires results (a group of experts giving their assessment to security situation in organization).

Fig. 4 shows the decomposition of the risk assessment process in providing data security of cloud computing.

As shown in Fig. 4, this process represents five consecutive stages: "Goal factors detection", "Threats identification", "Calculate threats consequences" "Calculate risk levels" and "Risk reduction recommendations development". Study object, for which CC risks are calculated, stands organization that uses a cloud service for its work (providing access to services to their users / customers).

First stage “Goal factors detection” includes two subprocesses: “Input data analysis” and “Define a set of goal factors”. Goal factors define and limit the observed events and processes in the CC and represent a list of key parameters, interpreted as a significant, important in cloud computing services usage process. According to Cloud Security Alli-

ance investigation results [9, 10] and our own development a set of goal factors for cloud computing risk assessment process (for SaaS and PaaS service models) was constructed (Table 1).

Decomposition of next stage, "Threats identification", is shown in Fig. 5. On this stage a set of elemental factors for every goal factor is defined and, depending on the results, a list of threats for every elemental, and respectively, every goal factor is detected.

Elemental factors represent more specific critical components of security, and subsystems, which goal factors consist of. Set of elemental factors for SaaS and PaaS service models was defined in analogous way, referring to experts' opinion (Table 2).

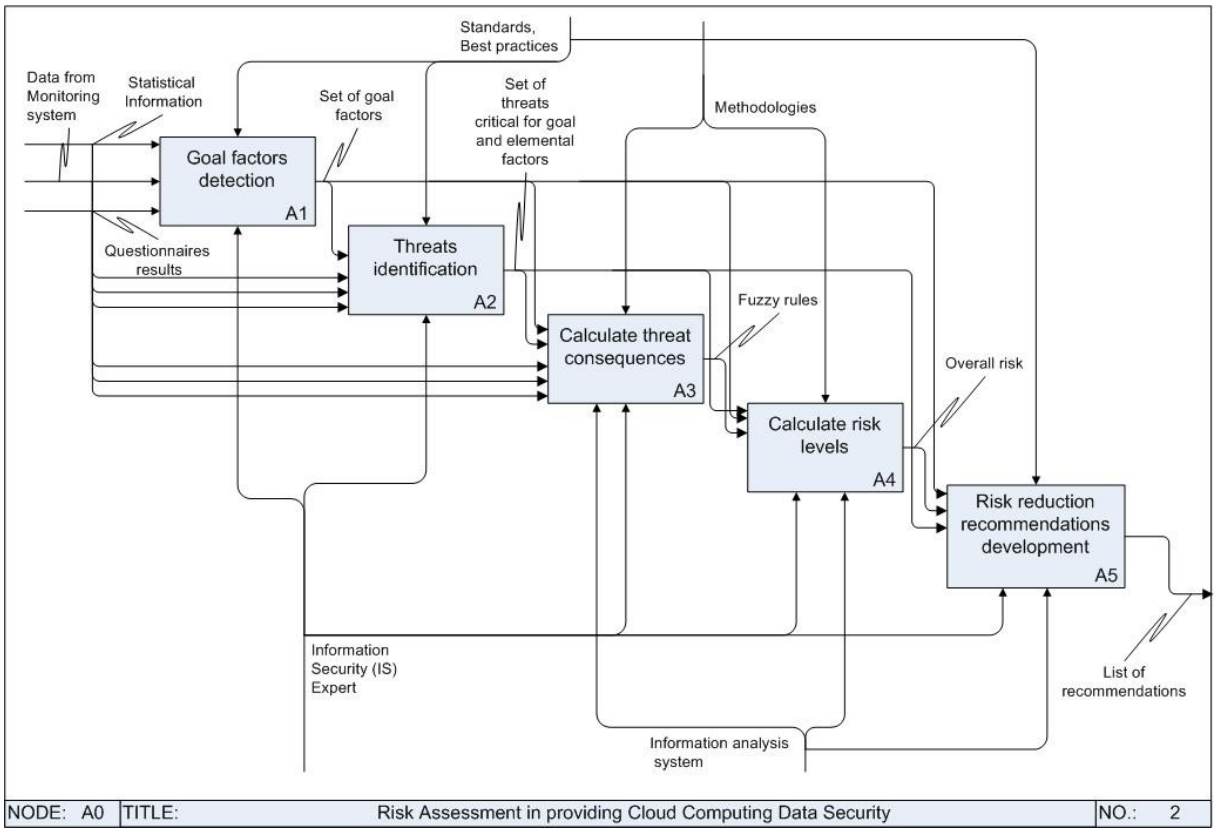


**Fig. 4.** Decomposition of CC risk assessment process

Table 1

**Set of goal factors for CC risk assessment process**

| № | Concept | Concept name | State variable, $x_i$ |
|---|---|---|---|
| 1 | $C_1^G$ | Compliance | Level of compliance of all systems and procedures |
| 2 | $C_2^G$ | Data Governance | Level of data control |
| 3 | $C_3^G$ | Human Resources | Level of human resources compliance |
| 4 | $C_4^G$ | Information Security | Level of information security |
| 5 | $C_5^G$ | Legal Compliance | Level of compliance with policies and regulations |
| 6 | $C_6^G$ | Operations Management | Level of operations management protection |
| 7 | $C_7^G$ | Identity and Access Management | Level of access security |
| 8 | $C_8^G$ | Risk Management | Level of protection according to risk management process |

In compliance with recent studies of National Institute of Standards and Technology (USA), Bundesamt für Sicherheit in der Informationstechnik (Germany), and others [4, 5, 8], a set of threats, which can bring serious damage to organizations' data, assets, profitability, reputation, etc. was defined. Fragment of threat list is shown in Table 3.

Third stage of risk assessment in providing CC data security, "Calculate threats consequences", include following subprocesses: "Create situational plans of threats realization", "Calculate threat realization damage cost", "Calculate indexes for each goal object factor", "Estimate the fuzzy logic model for each factor".

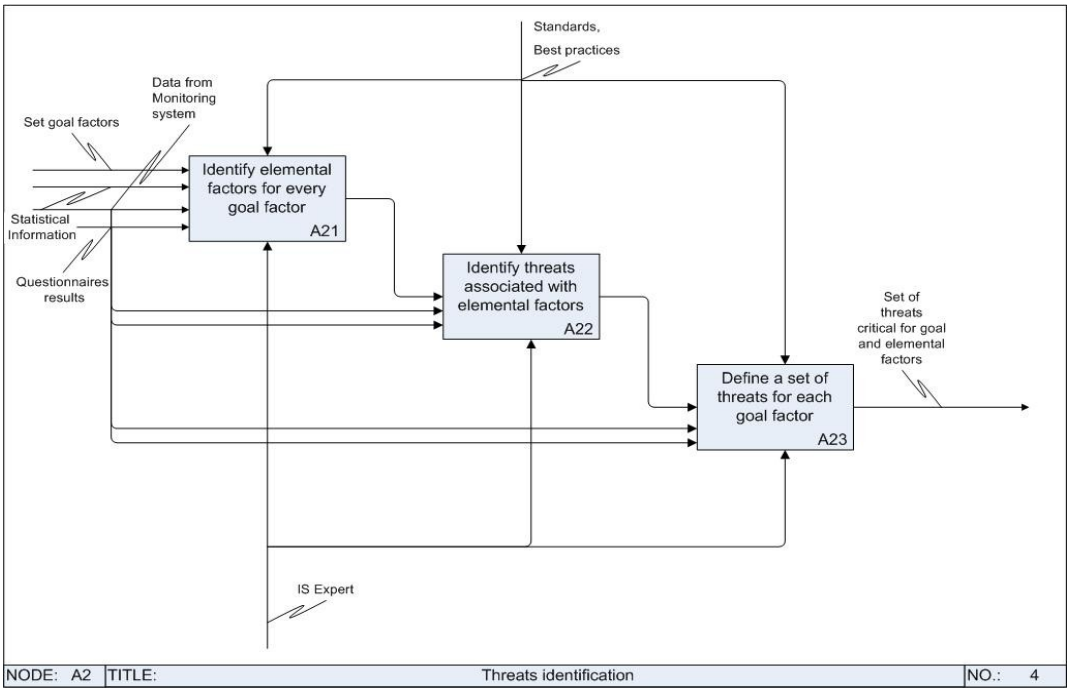


**Fig. 5.** Decomposition of "Threats identification" subprocess

Table 2

**Set of elemental factors for CC risk assessment process**

| Concept | Concept name | Concept | Concept name |
|---|---|---|---|
| $C_1^E$ | Antivirus / Malicious Software | $C_{11}^E$ | Employment |
| $C_2^E$ | Application Security | $C_{12}^E$ | Encryption |
| $C_3^E$ | Audit | $C_{13}^E$ | Equipment |
| $C_4^E$ | Authentication | $C_{14}^E$ | Incident Management |
| $C_5^E$ | Authorization | $C_{15}^E$ | Risk Mitigation / Acceptance |
| $C_6^E$ | Baseline Requirements | $C_{16}^E$ | Network / Infrastructure Services and Security |
| $C_7^E$ | Business Continuity | $C_{17}^E$ | Outsourced Development |
| $C_8^E$ | Data Security / Integrity | $C_{18}^E$ | Working Environment |
| $C_9^E$ | Documentation | $C_{19}^E$ | Roles / Responsibilities |
| $C_{10}^E$ | Disaster recovery | $C_{20}^E$ | Third Party Access and Service Level Agreements (SLA) |

Table 3

**Fragment of list of threats for CC risk assessment process**

| Concept | Concept name | State variable, $x_i$ |
|---|---|---|
| $C_1^T$ | Access Control Threats | The average number of incidents of unauthorized access |
| $C_2^T$ | Account, service or traffic hijacking | The average number of incidents of account, traffic or service hijacking |
| $C_3^T$ | Address spoofing | Presence of CM against address spoofing |
| $C_4^T$ | Application Vulnerabilities | Number of incidents of application failures |
| $C_5^T$ | Bot Network | Number of incidents from a bot network |
| $C_6^T$ | Data loss/leakage | Number of incidents of data loss/leakage |
| $C_7^T$ | Data storage threats | Compliance with data privacy standards |
| $C_8^T$ | Data transit threats | The average number of incidents of data modification |
| $C_9^T$ | Excess privileges / excessive access | The average number of detected facts of authority abuse |
| $C_{10}^T$ | Failure to meet Regulatory Compliance requirements | The number of negative audit reports |
| $C_{11}^T$ | Identity theft | The average number of identity theft attacks |
| $C_{12}^T$ | Inaccurate inventory | Not accounted data in information stream |
| $C_{13}^T$ | Insecure / vulnerable configurations | Network-layer, application-layer, local operating system-layer vulnerability scans monitoring |
| $C_{14}^T$ | Insecure processes | Number of processes described and followed |
| $C_{15}^T$ | Intrusion | The average number of intrusion attacks |
| $C_{16}^T$ | Lack of complete auditing | Number of audit checks in a year |
| $C_{17}^T$ | Lack of continuous monitoring | Availability of monitoring of key systems, %; percentage of accounted data about users, % |
| $C_{18}^T$ | Malicious activity | Presence of HR requirements in legal contracts; availability of security breach determination process, % |

The choice in favour of fuzzy systems has been made for the following obvious advantages:

• opportunity to operate with fuzzy input data, for example, continuous time-varying values (dynamic task), values that cannot be found single-valued (results of statistical surveys, advertising agencies, etc.);

• opportunity to formalize fuzzy evaluation criteria and make a comparison: manipulation of the criteria of "most," "may," "mostly";

• opportunity for qualitative estimates as input, and output results, i.e. ability to operate not only in the values data, but also their degree of reliability, and distribution;

• opportunity for fast simulation of complex dynamic systems and their comparative analysis with a given degree of accuracy.

According to fuzzy cognitive maps (FCM) theory, which we use in our research, represent a fuzzy oriented graph whose nodes are fuzzy sets. Directed edges of the graph, not only reflect causal relationships between factors, but also determine the degree of influence (weight) connects. Weights of the edges - it is either a number from the interval [– 1, 1], or the values of a linguistic scale type {Low, Medium, High}, which characterize the strength of influence relevant connection or degree rely on presence of this connection. Methods of analysis used FCM operations are fuzzy mathematics [11]. Example of fuzzy cognitive map for our investigation is shown in Fig. 6.

The most common approach to fuzzy influences calculation is the following: suppose that between factors $f_i$ and $f_j$ there are $m$ paths, and $I_r(f_i, f_j)$ denotes influence of $f_i$ on $f_j$ along $r$ path, and $T(f_i, f_j)$ aggregate influence of $f_i$ on $f_j$ along all $m$ paths. Then:

$$I_r(f_i, f_j) = \min_p w_{p,p+1}, \quad (1)$$

$$T(f_i, f_j) = \max_{1 \le r \le m} I_r(f_i, f_j), \quad (2)$$

where $w_{p,p+1}$ is weight of oriented graph of $f_p$ on $f_{p+1}$ along $r$ path. Thereby $I_r(f_i, f_j)$ highlights the most weak connection of $f_i$ on $f_j$ along $r$ path (1), and $T(f_i, f_j)$ highlights the most strong connection in $I_r(f_i, f_j)$ (2).

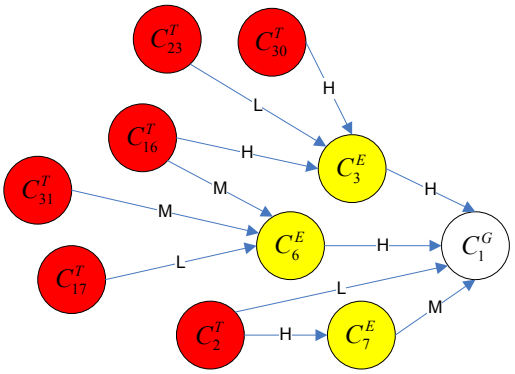


**Fig. 6.** Fuzzy cognitive map fragment

Weights of oriented graphs' paths named according to field research (e.g. network security, authentication) and experts' assessment results. Thus fuzzy logic model calculated for every goal factor of the cloud computing risk assessment process.

Next subprocess "Calculate risk level" represents four steps, as shown in Fig. 7.

The strongest connections in $I_r(f_i, f_j)$, which were mentioned above, will correspond to probability of threat realization. Thereby, information security relative risk value for each goal factor (subprocess A41 in Fig. 7) can be defined by the formula (3):

$$\overline{R_{C_1^G}} = T(f_i, f_j)\frac{K_{C_1^G}}{K_\Sigma}, \qquad (3)$$

where $\frac{K_{C_1^G}}{K_\Sigma}$ – relative cost of resource (e. g. "Compliance"), that can be defined by statistical information and expert knowledge. Then value of overall relative risk indicator (subprocess A42 in Fig. 7) can be found in the following way (4):

$$\overline{R} = \sum_{n=1}^{N} \overline{R}_{C_n^G} \qquad (4)$$

Next steps: estimation of similarity indexes and comparative analysis of obtained indicators provide levels of confidence, matter how calculated parameters are reliable.

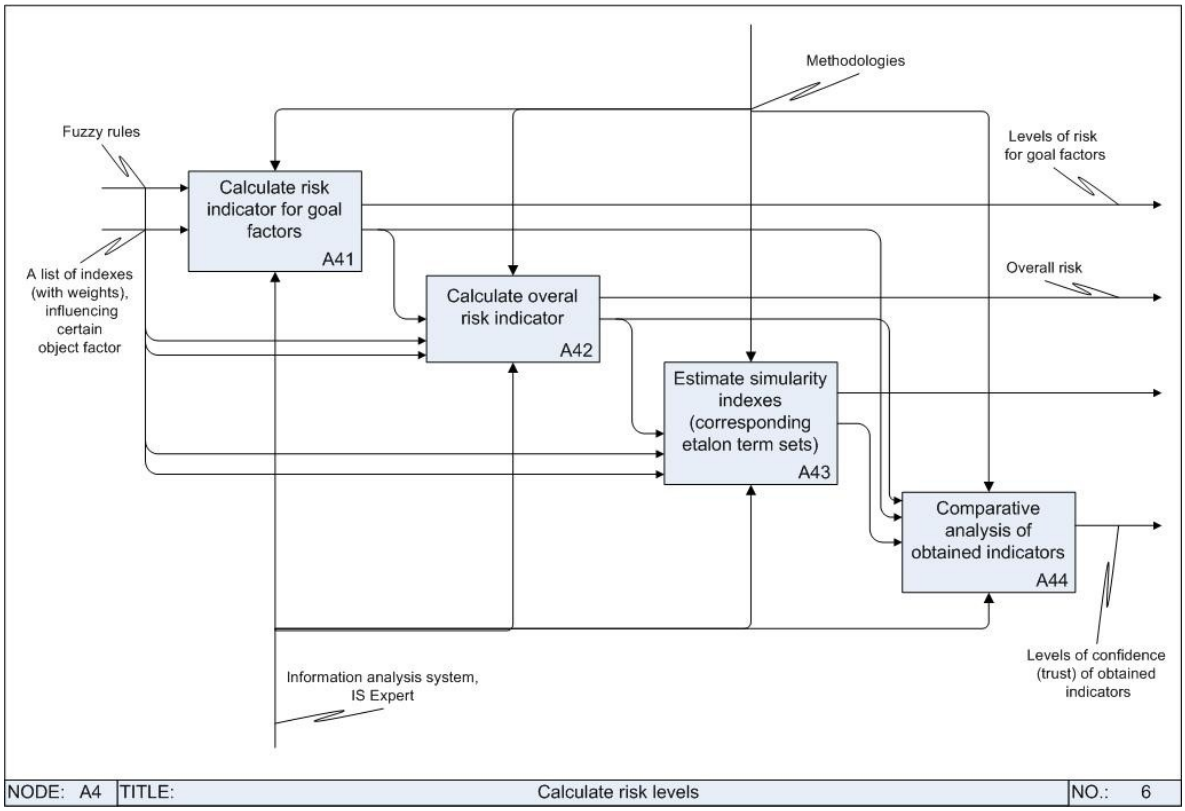


**Fig. 7.** Decomposition of "Calculate risk level" subprocess

Last stage of CC risk assessment process starts with determination of a list of recommendations to reduce the risk level, calculation of required resources (financial, material, human), continue with generation of a set of recommendations for possible actions of risk reduction and conduction ranking of recommendations according to the principle of priority. On last step system attaches instructions to eliminate the consequences in case of threat realization.

The results of the risk assessment process are recommendations on risk reduction and use of cloud services, which are formed in the information-analytical system. In addition to the recommendations the output data are the levels of risk, both general and individual, for each goal factor that correspond to a particular object on cloud computing security issues. This information can be used further to insure information security of the organization.

## 5. IMPLEMENTATION IN MATLAB (SIMULINK)

Consider the example of approach implementation in MATLAB (Simulink) environment.

Goal factor "Compliance" influenced by following elemental factors: "Audit", "Baseline requirements", and "Business Continuity". Example of FCM approach with 3 inputs and 1 output, constructed in MATLAB Fuzzy Toolbox, is shown in Fig. 8.

For each of input and output parameters it is necessary to specify membership functions (Fig. 9). The membership function (MF) of a fuzzy set is a generalization of the indicator function in classical sets. It represents the degree of truth as an extension of valuation. $MF(x) = 0$ represents absence of membership , and if $MF(x) = 1$, then it is case of full membership. There can be different types of MF (triangle, trapezoidal, gauss, etc.). E. g., trapezoidal MF is defined by 4 numbers *(a,b,c,d)* and her value in $x$ is determined according to equation (5):

$$MF(x) = \begin{cases} 1 - \dfrac{b-x}{b-a}, & a \le x \le b, \\ 1, & a \le x \le b, \\ 1 - \dfrac{x-c}{d-c}, & c \le x \le d, \\ 0, & \text{In other cases.} \end{cases} \quad (5)$$

In presented approach example, linguistic parameter for trapezoidal membership functions of output variable "Compliance" is assumed to be: {"Low", "Below average", "Average", "Above average", "High"}.

Also it is necessary to specify a set of rules in the form: IF-THEN. For example, in our case:

- if "Audit" is "Not accomplished", and "Baseline requirements" is "Not documented", and/or "Business continuity" is "Medium", then "Compliance" is "Low";
- if "Audit" is "Partially accomplished", and "Baseline requirements" is "Not documented", and "Business continuity" is "High", then "Compliance" is "Below average";
- if "Audit" is "Partially accomplished", and "Baseline requirements" is "Well documented", and/or "Business continuity" is "Medium", then "Compliance" is "Above average";
- if "Audit" is "Accomplished successfully", and "Baseline requirements" is "Fully documented", and "Business continuity" is "Low", then "Compliance" is "High"; etc.

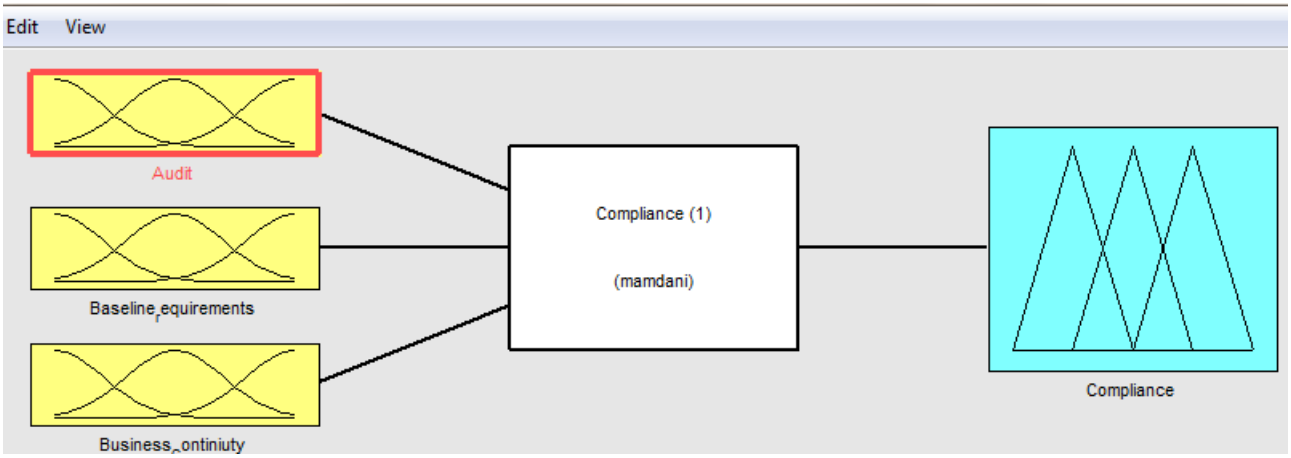


**Fig. 8.** Main window of MATLAB Fuzzy Toolbox

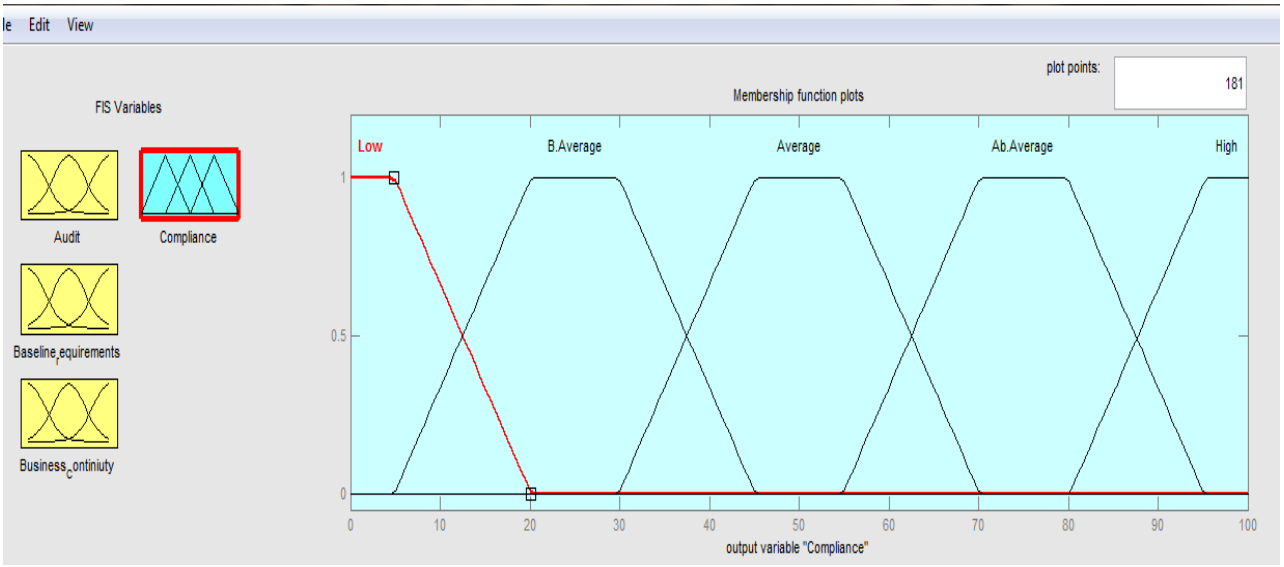


**Fig. 9.** Specifying membership functions for output parameter

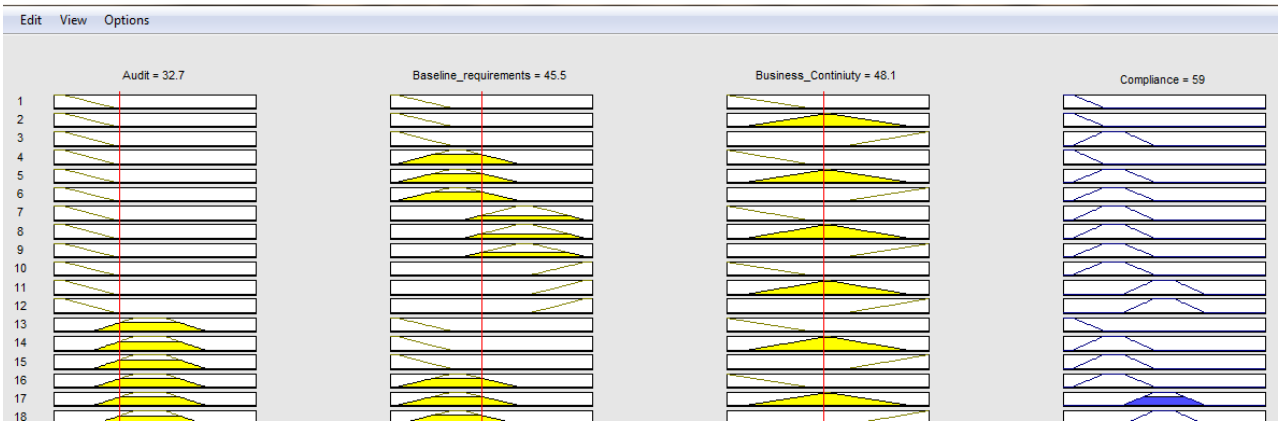


**Fig. 10.** Fuzzy logic toolbox result window

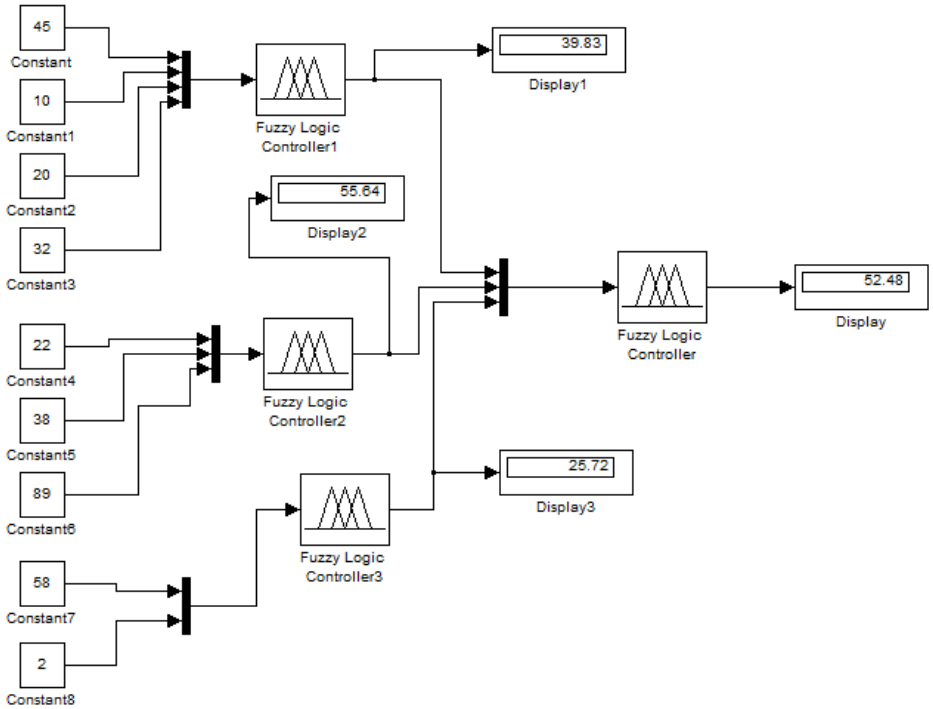


**Fig. 11.** Example of fuzzy logic controllers' implementation in Simulink

In case of realization of mentioned above rule example, “Compliance” membership functions will represent such a result in quantitative expression (Fig. 10). Thereby, goal factors’ “Compliance” value is 59, which corresponds to linguistic parameter “Average” with degree of membership equal 0,6 and to linguistic parameter “Above average” with degree of membership equal 0,25.

Thus fuzzy cognitive maps allow to look at the risk assessment process in providing data security while using cloud computing services from another point of view. Possibilities to consider all of the slightest “maybe” in experts’ knowledge open unique perspectives not to miss important aspects of information security in cloud computing.

## 5. CONCLUSION AND FUTURE WORK

In presented article the following tasks were completed:

• the definition of cloud computing, its basic models, services and security issues were presented;

• lists of main threats, basic and goal factors for CC were constructed;

• conceptual, functional and mathematical models for cloud computing security were constructed;

• solution for cloud computing threats identification using fuzzy cognitive maps were proposed;

• example of introduced approach embodied in MATLAB was presented.

The described process of risk assessment is important to ensure the security of cloud computing, of how to deploy different models of cloud and use them. Cloud computing technology meets the requirements of information security and analysis of all possible risk factors is needed, as for a user of these services and their providers.

Subsequent work will concentrate on more precise detailed study of factors and threats, investigation of other CC service and deployment models, as well as automation of the model information analysis system.

**ACKNOWLEDGMENTS**

This investigation is supported by the grant 12-07-00377-a of Russian Foundation for Basic Research, the research work has been performed within the state work on theme 8.1224.2011 «Development of software tools support decision-making for different kind of management activity in industry in the conditions semi structured data based on the technology of distributed artificial intelligence».

**REFERENCES**

1. Zhang Yandong, Zhang Yongsheng, “Cloud computing and cloud security challenges,” in *2012 Int. Symp. Information Technology in Medicine and Education*, 978-1-4673-2108-2112 IEEE.
2. Zaigham Mahmood, “Cloud computing: characteristics and deployment approaches,” *2011 11th IEEE Int. Conf. Computer and Information Technology*. 978-0-7695-4388-8/11 IEEE.
3. NIST SP 800-145. *The NIST Definition of Cloud Computing. Information Technology Laboratory*, National Institute of Standards and Technology, September 2011.
4. Fraunhofer Institute for Secure, Information Technology SIT. *On the Security of Cloud Storage Services*. March 2012.
5. BSI Standard 100-2 IT-Grundschutz Methodology. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008
6. Cloud Security Alliance. *Top Threats to Cloud Computing.* http://www.cloudsecurityalliance.org March, 2010.
7. Jianhua Che, Yamin Duan, Tao Zhang, and Jie Fan, “Study on the security models and strategies of cloud computing,” in *Procedia Engineering*, 23, pp. 586-593, 2011.
8. COBIT 5. *A Business Framework for the Governance and Management of Enterprise IT*.
9. Cloud Security Alliance. Cloud Control Matrix. Version 1.3. Sept., 2012. Available: https://cloudsecurityalliance.org/research/ccm
10. Hamid Tohidi, “The role of risk management in IT systems of organizations,” in *Procedia Computer Science*, 3, pp. 881–887, 2011.
11. I. M. Azhmuhamedov, *Information Security Challenges Based on System Analysis and Fuzzy Cognitive Modeling*, (in Russian). Astrakhan, 2012.

**ABOUT AUTHORS**

**KONRAD, Uwe**, Head of department of information technology in Helmholtz Zentrum Dresden-Rossendorf (HZDR), Dresden, Germany.

**PENZINA, Vladislava**, Postgrad. (PhD) Student, Dept. of Computational Mathematic and Cybernetics. Dipl. mathematician and economist (UGATU, 2010).