ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES / Index A LOS AUTORES / To the AUTORS

Vol. 40 (Number 18) Year 2019. Page 16

A fuzzy mathematical model for managing the digital transformation of business processes based on cloud services

Un modelo matemático difuso para gestionar la transformación digital de los procesos de negocio basados en servicios en la nube

KORABLEV, Anton V. 1 & PETRUSHOVA, Marina V. 2

Received: 27/02/2019 • Approved: 14/05/2019 • Published 03/06/2019

Contents

ABSTRACT:

This paper investigates the implementation of technological innovations as illustrated by cloud-based service provision. The paper proposes a method based on the mathematical tools of fuzzy logic and designed for modelling information-security risks involved in the use of cloud technology. We have developed an approach for mathematically analysing the components of information-security risks inherent in the use of cloud technology. The approach differs from others in that the proposed set-theoretical risk model incorporates an adaptive analytical model for organising cloud technology at a company with due regard to the many information-based relationships between information resources and vulnerabilities. We have introduced an integrated systematisation of information-security risks involved in the digital transformation of business processes. That systematisation factors in the nuances of cloud technology, provides a high level of detail, and makes for accurate forecasting of information-security risks relating to provision of cloud services. We have given a rationale for the statement of the problem of fuzzy mathematical modelling of information-security risks

RESUMEN:

Este documento investiga la implementación de innovaciones tecnológicas como lo ilustra la provisión de servicios basados en la nube. El documento propone un método basado en las herramientas matemáticas de lógica difusa y diseñado para modelar los riesgos de seguridad de la información involucrados en el uso de la tecnología de la nube. Hemos desarrollado un enfoque para analizar matemáticamente los componentes de los riesgos de seguridad de la información inherentes al uso de la tecnología en la nube. El enfoque difiere de otros en que el modelo de riesgo teórico de conjuntos propuesto incorpora un modelo analítico adaptativo para organizar la tecnología de nube en una empresa, teniendo debidamente en cuenta las numerosas relaciones basadas en información entre los recursos de información y las vulnerabilidades. Hemos introducido una sistematización integrada de los riesgos de seguridad de la información involucrados en la transformación digital de los procesos de negocios. Esa sistematización tiene en cuenta los matices de la tecnología de la nube, proporciona un alto nivel de detalle y permite un pronóstico preciso

using an expanded criterion set. The risk-determination model includes standard parameters for risk probability supplemented by the fuzzy boundaries of resource value and of the impact the risk has on basic business processes. This paper also proposes a method for determining indicators characterising corporate information-security risks both from the perspective of potential economic consequences and from that of the value of a given information resource.
Keywords: digital transformation, information-security risk, cloud technology, fuzzy sets

de los riesgos de seguridad de la información relacionados con la provisión de servicios en la nube. Hemos dado una justificación para explicar el problema del modelado matemático difuso de los riesgos de seguridad de la información utilizando un conjunto de criterios expandido. El modelo de determinación de riesgos incluye parámetros estándar para la probabilidad de riesgo complementada por los límites difusos del valor del recurso y del impacto que el riesgo tiene en los procesos básicos del negocio. Este documento también propone un método para determinar los indicadores que caracterizan los riesgos corporativos de seguridad de la información tanto desde la perspectiva de las posibles consecuencias económicas como desde el valor de un recurso de información dado.
Palabras clave: transformación digital, riesgo de seguridad de la información, tecnología de nube, conjuntos difusos.

1. Introduction

Digital transformation based on corporate innovation-driven development builds on a set of various technological, organisational, managerial, social, information, and communication innovations. Implementing innovations consists, first and foremost, in using advanced information technology, making it possible to solve several major problems such as improving companies' competitiveness and staff efficiency, developing economically viable lines of business as a top priority, and transforming customer interaction to improve customer loyalty.

In particular, today client and supplier management requires creating and correctly using new forms of information exchange based on modern remote technologies. One such technology is virtualising the exchange of information between clients and staff—that is, providing services as cloud services.

Most modern companies are distributed systems with well-developed telecommunication infrastructures. Here, the principal purpose of information technology is for all of the company's business units to operate in a single information environment using up-to-date, accurate data across the company (Ebrahimzadeh & Najafi & Alavidoost, 2016). This is achievable by using cloud services.

In the economic field, managerial decision-making involves the use of asymmetrical, incomplete, or restricted information. All these negative properties of information cause various threats and risks that go hand in hand with the company's operations.

Digital transformation of business processes involves risks inherent in the use of supporting information technology. Because of this, solving the problem of efficiently managing information-security risks has an effect on the implementation and use of innovations by companies (Galbusera &Giannopoulos, 2018).

Even as the significance of information support grows, modern management techniques are beginning to incorporate a new, risk-oriented approach to managing the collection, processing, storage, and transfer of information. That this approach has emerged is due to the following qualitative changes that have taken place in information management: Corporate financial losses from incidents related to information security have increased dramatically. Companies are now spending more to create, use, and improve their IT infrastructures. Up to 20% of financial expenditure for developing and implementing new information technology is channelled to solving issues related to information protection (Geras'kin, 2018), (Geras'kin & Chkhartishvili, 2017).

2. Methodology

Information-security threats also affect cloud services, which are traditionally based on hardware, software, and organisational management techniques used in network interaction. This causes vulnerabilities specific to cloud technology. As a result, a single approach needs

to be developed to identify components of the information-security risk related to the use of cloud technology as part of digital transformation of business processes, based on a mathematical set model. The use of this approach will help develop a method for determining the final potential economic loss, costs related to countering threats, the value of the information resource in question, and quantified risks. The basis of the method is a model for fuzzy assessment of information-security risks (D'Urso & De Giovanni & Massari, 2018), (Klöber-Koch & Braunreuther, 2018). Unlike conventional management models, this model determines values for components of cloud technology by those of their properties that directly influence the level of information-security risks.

The wide variety of specific information-security threats typical of cloud technology requires developing an adequate method for monitoring and assessing the status of information-security risks involved in the use of cloud services at the company. For purposes of solving the problem stated, a generalised formal algorithm has been developed for fuzzy assessment of information-security risks related to cloud technology. The proposed method is based on the mathematical tools of fuzzy-set theory. This made it possible to determine the form of presenting the cloud-technology model, formulate an algorithm for assessing information-security risks, the amount of loss, the probability of a specific threat being carried out, and countermeasures taken.

In essence the method complies with the recommendations of the international standard NIST SP 800-39 for managing information-security risks (Anbari & Tabesh & Roozbahani, 2017), (Alfonso & Roldán, 2017). The algorithm consists of six stages that are dividable, for purposes of this discussion, into two related groups.

Group 1 stages involve describing and shaping a cloud-technology model. This includes steps to determine characteristics of the model’s elements as well as listing, and defining the composition of, what information-security risks comprise.

Group 2 stages involve calculating the magnitude of information-security risks and assessing those risks. Data from the preceding stages are used in computing the amount of loss and the probability that threats to protected information are carried out as well as for risk quantification. Results from this stage are presented as recommendations for managing risks at the company.

To formalise the cloud-technology model, one needs to determine its elements. These include corporate information resources, software and hardware, network equipment (routers, terminals, and concentrators), users (staff, clients, and violators), and steps to counter information-security threats and vulnerabilities, presented as regulatory and reference documents (Masneva & Petrushova, 2016), (Luo & Hu, 2015).

Using the premises of system and system-analysis theory, we will present cloud technology as the set model

$$S = \{D,U,V,R\}, \qquad (1)$$

where represents information resources given as a set of components , . Resources are characterized by the fuzziness of information properties (confidentiality, continuity, and availability). The composition of information resources corresponding to cloud technology is determined jointly by the company’s technical and business staff.

 represents threats typical of cloud technology, and they are presented as a set of objects , . All detected threats are grouped by the type of impact on the properties of protected information.

 represents vulnerabilities typical of cloud technology, and they are presented as a set of objects , .

 represents typical information links between the components of cloud technology. Generally, the links can be written as , where .

It is noteworthy that the adequate cloud technology model is obtainable only after object sets and information links between its elements are determined.

Below we will determine the types of information links.

1. Interaction between information resources:

$$INTERACTION_D(d_1 d_2) = \begin{cases} 1 \text{ if resources are linked} \\ 0 \text{ if there is no interaction} \end{cases}$$

2. Interaction between information resources and threats:

$$INTERACTION_\Gamma(d_1 u_1) = \begin{cases} 1 \text{ if interaction takes place} \\ 0 \text{ if there is no interaction} \end{cases}$$

3. Interaction between threats and related vulnerabilities:

$$INTERACTION_V(u_1 v_1) = \begin{cases} 1 \text{ if interaction takes place} \\ 0 \text{ if there is no interaction} \end{cases}$$

When the premises and mathematical tools of fuzzy-set theory are used to describe and formulate a model for information-security risks, additional object sets—measuring scales and assessment functions—must be determined. A set of objects that represent measuring scales can be fuzzy, discrete, or continuous (Korablev, 2016), (Montanari & Bottani & Shekarian, 2017). Existing functions for fuzzy assessment of information-security risks can be used as a set of assessment functions.

The level of information-security risks in the model under study depends on the many external and internal factors that have an effect on the model. This necessitates determining the limits of interval values for components of information-security risks: information resources, vulnerabilities, and threats. For that purpose, defuzzified values are calculated for model elements by using properties that directly influence the level of information-security risk—that is, continuity, availability, and confidentiality (Sheehan & Gough, 2015).

The confidentiality of an information resource is characterised by the property value of element d in model S on the fuzzy measuring scale S_{conf}. The defuzzification function $Defuzzy(S_{conf})$ is used to calculate crisp interval values.

The continuity of an information resource is characterised by the property value of element d in model S on the fuzzy measuring scale S_{cont}. The defuzzification function $Defuzzy(S_{cont})$ is used to calculate crisp interval values.

The availability of an information resource is characterised by the property value of element d in model S on the fuzzy measuring scale S_{avail}. The defuzzification function $Defuzzy(S_{avail})$ is used to calculate crisp interval values.

To make the model more adequate, one must also determine the value level of the information resource. We will express the value $VALUE(d_n)$ as the criticality level of element d for model S. Here the fuzzy measuring scale S_{value} is used. The criticality category depends on the aggregate value of the properties of confidentiality, continuity, and availability. The defuzzification function $Defuzzy(S_{value})$ is used to calculate crisp interval values, and here $Defuzzy(S_{\text{value}}) = D$.

We will determine the total value of the model's elements—that is, the ultimate importance of information resources—with the expression

$$VALUE_S = \sum_{n=1}^{m} VALUE(d_n), \tag{2}$$

where m is the total quantity of model elements and n is the information resource.

Also important is the relative value of information resource d for the model as a whole, and it is expressed as the final value of the [0–1] range.

$$RELATIVE\_VALUE(d_n) = \frac{\cos t(d_n)}{VALUE_s}. \tag{3}$$

A primary characteristic of the level of information-security risk is the category of loss from threats specific to the model under study (Groumpos, 2015), (Henriquesde & Camarae, 2016).

Let us determine the value of potential loss $LOSS(d_n)$ subject to the information resource targeted by the threat. The impact of information resource d on the model's interrelated elements is fuzzy: $INFLUENCE(d, d_n)$. The membership degree (d, d_n) is determined by an expert using a linguistic variable on the effect scale S_{effect}, and it denotes a fuzzy relationship between the information resource and the threat and the related vulnerability. We will note that $INFLUENCE(d, d_n)$ = 0 if one of the pair's elements is not connected with the other element and that $INFLUENCE(d, d_n)$ = 1 if one of the pair's elements has the largest effect on the amount of loss for the other element.

$$LOSS(d_n) = \sum RELATIVE\_VALUE(d_n) * INFLUENCE(d, d_n), \tag{4}$$

The identified fuzzy measuring scales S_{conf}, S_{cont}, and S_{avail} will make it possible to determine the value of potential loss from the information resource $LOSS(d_n)$ by its properties of continuity, availability, and confidentiality.

Potential loss from the information resource subject to continuity:

$$LOSS_{cont}(d_n) = Defuzzy(S_{cont}) * LOSS(d), \quad (5)$$

Potential loss from the information resource subject to availability:

$$LOSS_{avail}(d_n) = Defuzzy(S_{avail}) * LOSS(d), \quad (6)$$

Potential loss from the information resource subject to confidentiality:

$$LOSS_{conf}(d_n) = Defuzzy(S_{conf}) * LOSS(d), \quad (7)$$

Assessing the significance of potential loss from the information resource and of aggregate loss requires the use of the logical-sum operation. In this case, the gross loss is calculated with the equation

$$LOSS_S = \sum_{n=1}^{m} \circ LOSS(d_n), \quad (8)$$

The identified fuzzy measuring scales S_{conf}, S_{cont}, and S_{avail} will make it possible to determine the total value of potential loss from information resources $LOSS(d_n)$ by their properties of continuity, availability, and confidentiality.

The total value of potential loss subject to continuity:

$$LOSS_{cont} = \sum_{n=1}^{m} \circ LOSS_{cont}(d_n), \quad (9)$$

The total value of potential loss subject to availability:

$$LOSS_{avail} = \sum_{n=1}^{m} \circ LOSS_{avail}(d_n), \quad (10)$$

The total value of potential loss subject to confidentiality:

$$LOSS_{conf} = \sum_{n=1}^{m} \circ LOSS_{conf}(d_n), \quad (11)$$

Calculating the total value of the fuzzy information-security risk subject to the value of information resources for the model under study requires the use of the logical-sum operation.

$$INF\_RISK_{\text{val}}(S) = INF\_RISK_{fuzzy}(S) \circ VALUE, \quad (12)$$

We will assess the fuzzy information security-risk with the full set of S-conorms and T-norms.

A verbal description of the linguistic variable of the model's information-security risk on the fuzzy scale of aggregate risk:

$$INF\_RISK_L = Fuzzy(IR(S), S_{risk}), \quad (13)$$

This set includes three options with three values each, totalling nine values for $INF\_RISK(S)$ in the [0–1] range.

3. Results

This discussion analyses the Virtual Office cloud service. The set model for cloud technology will contain sets of elements: a user terminal, a network gateway, a virtualisation server, a web server, a database server, remote attacks on cloud-infrastructure components, DDOS attacks, software or hardware faults at the provider, the provider's noncompliance, the provider's failure to destroy information, loss of communication with the provider, insiders at the provider, and account data hacked as part of authorisation and authentication.

For the identified elements of the model, experts have determined fuzzy relationships needed to assess the level of information-security risks by using fuzzy measuring scales: confidentiality, the degree of impact on resources, and loss.

Using equations (5) through (8), we determined the loss the company may sustain in countering information security threats (see table 1).

Table 1
Costs related to countering threats

	Loss							
Resources								
	LP	LS	LP	LS	LP	LS	LP	LS
	0.1459	0.043	0	0.143	0.132	0.323	0	0.125
	0.1254	0.212	0	0.042	0.111	0.046	0.111	0.112
	0	0.035	0	0.544	0	0.076	0	0.024
	0	0.041	0	0.045	0	0.452	0	0.231
	0.1423	0.434	0	0.045	0	0.037	0	0.113
	0.1111	0.046	0	0.041	0	0.034	0	0.136
Total loss	0.5247	0.811	0	0.86	0.243	0.968	0.111	0.741

Source: compiled by the authors

The calculation involves the use of dual fuzzy operations: logical product (LP) and logical sum (LS). Defuzzification involves the use of the centre-of-gravity method (some integrals are determined analytically). Fuzzy negation uses subtraction from 1.

The linguistic values of information-security risks related to continuity ('Unauthorised change of information' and 'Change of services provided') are determined:

$$Fuzzy(0,32; S_{\text{risk}}) = \text{High (H)}$$

$$Fuzzy(0,73; S_{\text{risk}}) = \text{Critical (C)}$$

The linguistic values of information-security risks related to availability ('Business shutdown,' 'Loss of control over data,' and 'Service suspension') are determined:

$$Fuzzy(0,76; S_{\text{risk}}) = \text{Critical (C)}$$

$$Fuzzy(0,87; S_{\text{risk}}) = \text{Superhigh (SH)}$$

The linguistic values of information security risks related to confidentiality ('Information leak,' 'Illicit access,' Unauthorised access to information,' 'Information theft') are determined:

$$Fuzzy(0,74; S_{\text{risk}}) = \text{Critical (C)}$$

As peak values are assumed by information-security risks related to availability, management should first of all focus on those risks when implementing the Virtual Office cloud service.
Quantitative indicators of information-security risks calculated with the mathematical tools of fuzzy sets are the values of the arithmetic mean risk $IR_{aver}(S)$ = 0.701 and the quadratic mean risk $IR_{aver}(S)$ = 0.775.

We will note that with this modelling method, information-security risks can be estimated for each information resource in the cloud service. This will make the safe use of information technology more efficient.

4. Conclusions

This article proposed a method for managing information-security risks that is based on the mathematical tools of fuzzy logic. This method can find application in situations where a company uses information technology with limited statistical data on information-security incidents.

An advantage of the method is that the "Risk" output variable yields a numerical value. This helps management make timely decisions in managing information technology.

Given that the implementation of innovations is based on information technology, efficient corporate innovation is conditional upon information security maintained at an acceptable level.

Bibliographic references

Alfonso, G., Roldán, C. (2017). A fuzzy regression model based on finite fuzzy numbers and its application to real-world financial data. *Journal of Computational and Applied Mathematics*, vol. 318, pp. 47-58.

Anbari, M.J., Tabesh, M., Roozbahani, A. (2017). Risk assessment model to prioritize sewer pipes inspection in wastewater collection networks. *Journal of Environmental Management*, vol. 190, pp. 91-101.

D'Urso, D., De Giovanni, L., Massari, R. (2018). Robust fuzzy clustering of multivariate time trajectories. *International Journal of Approximate Reasoning*, vol. 99, pp. 12-38.

Ebrahimzadeh, H., Najafi, S.E., Alavidoost, M.H. (2016). A novel fuzzy network SBM model for data envelopment analysis: A case study in Iran regional power companies. *Energy*, vol. 112, pp. 686-697.

Galbusera, L., Giannopoulos, G. (2018). On input-output economic models in disaster impact assessment. *International Journal of Disaster Risk Reduction*, vol. 30, pp. 186-198.

Geras'kin, M.I. (2018). Modeling Reflexion in the Non-Linear Model of the Stakelberg Three-Agent Oligopoly for the Russian Telecommunication Market. Automation and Remote Control, vol. 79. pp. 841-859.

Geras'kin, M.I., Chkhartishvili A.G. (2017). Structural modeling of oligopoly market under the nonlinear functions of demand and agents' costs. *Automation and Remote Control*, vol. 78, pp. 332-348.

Groumpos, P. (2015). Modelling Business and Management Systems Using Fuzzy Cognitive Maps: A Critical Overview. *IFAC-Papers On Line*, vol. 48, pp. 207-212.

Henriquesde, A.P., Camarae, G.L. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, vol. 36, pp. 25-34.

Klöber-Koch, L., Braunreuther, S. (2018). Approach For Risk Identification And Assessment In A Manufacturing System. Procedia CIRP, vol. 72, pp. 683-688.

Korablev, A.V. (2016). Application of cloud technologies in banking activities. *Journal of Economy and Entrepreneurship*, vol. 73, pp. 463-468.

Luo, J., Hu, Z. (2015). Risk paradigm and risk evaluation of farmers cooperatives' technology innovation. *Economic Modelling*, vol. 44, pp. 80-85.

Masneva, M.F., Petrushova, M.V. (2016). Internet portals of remote public services. *Journal of Economy and Entrepreneurship*, vol. 67, pp. 130-133.

Montanari, R., Bottani, E., Shekarian, E, (2017). A model for the analysis of procurement strategies in the economic order interval environment. *Mathematics and Computers in Simulation*, vol. 134, pp. 79-98.

Sheehan, T., Gough, M. (2015). A platform-independent fuzzy logic modeling framework for

environmental decision support. *Ecological Informatics*, vol. 34, pp. 92-101.

1. Candidate of Economic Sciences, Associate Professor of the Department of Corporate Information Systems, Electronic Services and Intelligent Information Technologies. Samara State University of Economics. E-mail: korablyov.av@gmail.com

2. Lecturer of the Department of Corporate Information Systems, Electronic Services and Intelligent Information Technologies. Samara State University of Economics. E-mail: tyri@yandex.ru

Revista ESPACIOS. ISSN 0798 1015
Vol. 40 (Nº 18) Year 2019

[Index]