Intelligent Information Management, 2015, 7, 230-241
Published Online July 2015 in SciRes. http://www.scirp.org/journal/iim
http://dx.doi.org/10.4236/iim.2015.74018

Development of Fuzzy Risk Calculation Method for a Dynamic Federation of Clouds

Rasim Alguliyev, Fargana Abdullayeva

Institute of Information Technology, ANAS, Baku, Azerbaijan
Email: director@iit.ab.az, farqana@iit.ab.az

Received 3 June 2015; accepted 25 July 2015; published 28 July 2015

Abstract

This paper suggests an approach for providing the dynamic federations of clouds. The approach is based on risk assessment technology and implements cloud federations without consideration of identity federations. Here, for solving this problem, first of all, important factors which are capable of seriously influencing the information security level of clouds are selected and then hierarchical risk assessment architecture is proposed based on these factors. Then, cloud provider's risk priority vectors are formed by applying the AHP methodology and fuzzy logic excerpt type risk evaluation is carried out based on this vector.

Keywords

Cloud Computing, Federation, Risk Assessment

1. Introduction

Large-scale distributed systems, such as cloud technologies, usually require interaction among various entities [1] [2]. In most cases, these entities belong to different network domains governed under different security policies. In cloud environment, interactions are achieving by federating of clouds [3] [4]. Federation is one of the main principles of cloud technologies [5].

In scientific research works, the problem of cloud federations is usually solved using identity federations. This solution, nevertheless, is not optimal, since identity federations have a number of problems: necessity of trust agreements, limited scalability, information security, privacy, identity provider detection problem, and interoperability [6] [7]. Besides, in [8] the authors claim that the federated identity management models (e.g., SAML) have problems regarding trust models that must be pre-established.

These problems of existing federation technologies make them inadequate for cloud environment, because the cloud environment is governed by uncertainty. It is necessary to establish an interaction between two unknown

How to cite this paper: Alguliyev, R. and Abdullayeva, F. (2015) Development of Fuzzy Risk Calculation Method for a Dynamic Federation of Clouds. *Intelligent Information Management*, **7**, 230-241. http://dx.doi.org/10.4236/iim.2015.74018

entities, in which no pre-established trust relations between them may arise.

To overcome this problem, a set of guidelines claim the necessity of developing methods which can provide an ad-hoc dynamic federation of clouds [9].

Ad-hoc federation is usually provided by assessing the risk level of federation party's identity infrastructure. For this purpose, in [10], it is claimed that the use of risk metrics can successfully eliminate the problem of circle of trust in existing federation systems and here a set of metrics are also proposed, organized in a taxonomy, which can be used in identity federations in the clouds. In [7], on the basis of risk-based access, control model is a developed federation model which is capable to establish the cloud federation without consideration of identity federations. Drawbacks of this approach are that it tries to describe the general situation of risk based federation, but there are no attempts to build a perfect risk computation model.

Several efforts are underway to standardize cloud security risk assessment, including the Cloud Security Alliance (CSA) [11] and European Network and Information Security Agency (ENISA) [12].

However, the CSA and ENISA efforts do not address how such assessments will be implemented as an automated service in a cloud environment. They also leave open the question of how a cloud consumer will build a test and development environment that includes security regression testing as well as assessment controls.

The suggested paper proposes a method that can provide federation of clouds without consideration identity federation, but allowing the possibility, of using it. This approach is based on risk assessment technology. For this purpose, a risk assessment method is proposed through a combination of Analytical Hierarchy Process (AHP) methodology and Mamdani fuzzy inference algorithm.

The main difference between our approach and the existing methods is the use of fuzzy risk model to enable the implementation of cloud federations. Here cloud federation is not carried to identity federation issues and implemented directly on the basis of infrastructure assessment.

2. Problem Statement

Various risk metrics are used for the establishment federation of clouds. In [10], Kabarkos defined a set of metrics, organized in a taxonomy, which can be used in the establishment of identity federations in the cloud. But only identity federation metrics are not considered sufficient for cloud federation [7]. For this purpose, it is necessary to consider the metrics serving to break the security level of the cloud infrastructure. Based on [13], risk factors which may damage the cloud security level include multi-tenancy related risks, administrative access risks, jurisdiction etc. Summarizing all of these, the main factors which can create greater risk to the security of the cloud provider can be classified as data security and privacy risks, organizational risks, technical risks, compliance and audit risks, physical security risks.

These factors they can also be grouped based on several aspects. One of the aspects is the legal nature of factors, and another is their technological nature. Governed by this approach risk factors of clouds can be classified as **Figure 1**.

As a result of such classification two inputs are formed for the last block: risks related to the technological problems of the clouds and risks related to the legal problems of the clouds.

The overall risk assessment system described in the form of a hierarchical structure is composed of separate subsystems which are organized as decision-making systems. Here inputs of one subsystem transmit the output signals to the input of the next decision-making system. This idea can be described as **Figure 2**.

Thus, according to various criteria these components are combined forming a general risk assessment system. Here input risk factors assigned to the decision block are described by the fuzzy sets, such as low, medium, high and some of the risk factors have a differently weighted role in the system. Here first of all, weighted factors are forwarded to the input of the decision-making system; weighted rules are established on these factors and obtained results forwarded to the next phase of the inference process. Here the goal is to forward a weighted input vector to the system. Decision making systems are described by "If … Then" type rules. Thus, a risk assessment method is proposed based on the collaborative decision-making theory.

The goal in determining the factor's weights is to achieve accuracy in the risk assessment process. For this purpose, weight ratios were calculated using the AHP methodology for each factor.

3. Analytical Hierarchy Process Methodology

The concept of AHP was developed, by Thomas Saaty in the 1970s. AHP is a decision making approach that

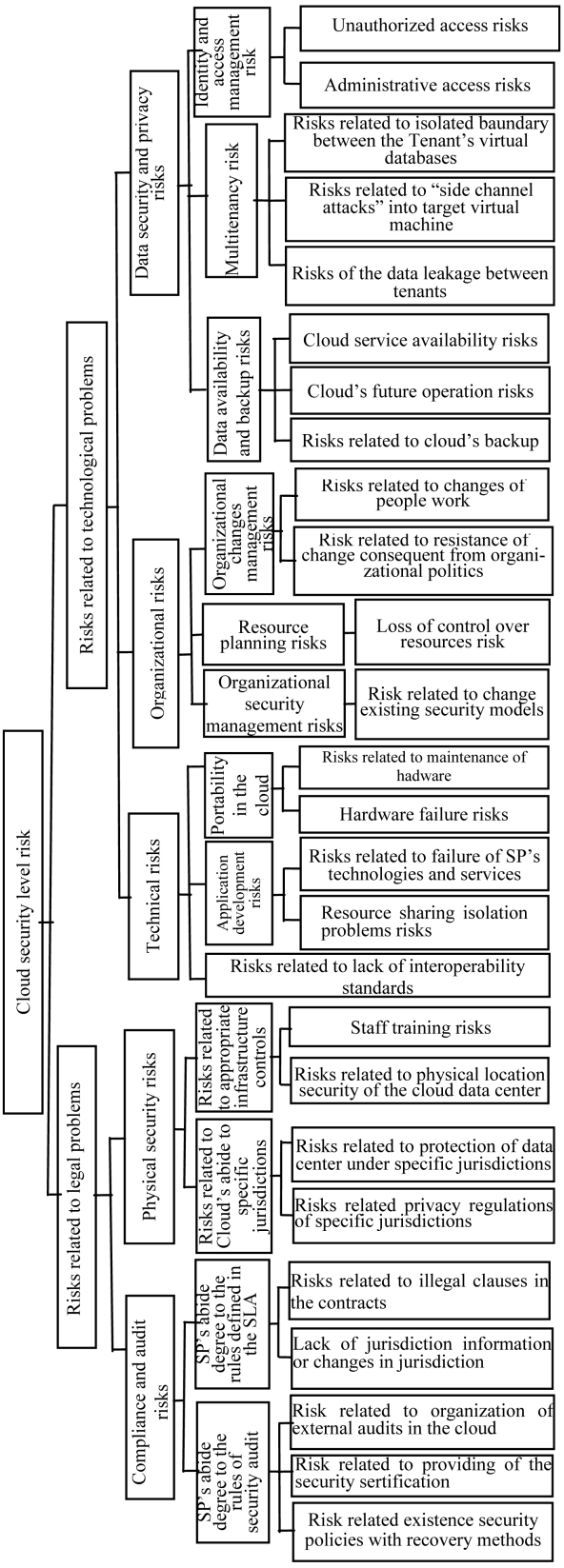

Figure 1. Classification scheme for cloud security risk factors.

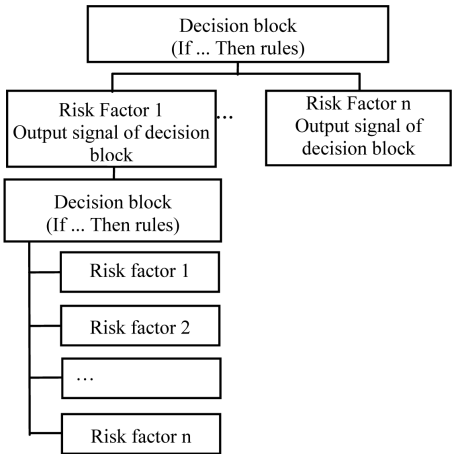

Figure 2. Hierarchical risk assessment structure.

involves structuring multiple choice criteria into a hierarchy, assessing the relative importance of these criteria, comparing alternatives for each criterion, and determining an overall ranking of the alternatives [14]. By organizing and assessing alternatives against a hierarchy of multifaceted objectives, AHP allows a better, easier, and more efficient identification of selection criteria, their weighting and analysis [15].

AHP algorithm is interpreted as follows:

Step 1. Development of decision making hierarchy. As shown in **Figure 1**, our study suggests a five-layered hierarchical structure. The objective, placed in level 1 of the hierarchy is the provider's risk value. Second level of hierarchy includes 2, and third level includes 5 factors, that enter into these decisions: data security and privacy risks, organizational risks, technical risk, compliance and audit risks, physical security risks. The next layer of the hierarchy is sub factors of the main factors.

Step 2. Establishment of comparison matrix for each layer. In this step, establishment of dominance rates matrix is carried out, based on a 9-point system ranging from 1 to 9.

$$A = \left[a_{ij} \right]_{n \times n} \tag{1}$$

where, a_{ij} is upper diagonal elements of the comparison matrix, $a_{ji} = \dfrac{1}{a_{ij}}$ lower diagonal elements of the comparison matrix.

Step 3. Establishment of normalized pairwise comparison matrix. Normalized comparison matrix is determined by dividing each element of the matrix A by its column total. Assume the sum of j-th column elements is $\sum_{i=1} a_{ij}$, then

$$a_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \tag{2}$$

Step 4. Calculation of weight vectors for the factors. Weight vectors of factors are determined by averaging the elements on each row of normalized comparison matrix. Weight ratio of row i is calculated as follows:

$$w_i = \frac{\sum_{j=1}^{n} a_{ij}}{n} \tag{3}$$

where n is the number of factors and weight ratios of factors are calculated as in **Tables 2-19**.

Step 5. Calculation of principal Eigen value. Principal Eigen value is obtained from the summation of products between each element of weight vector and the sum of columns of the decision matrix A.

$$\lambda_{\max} = \sum_{i=1}^{n} w_i \times a_{ij} \tag{4}$$

Table 1. Numbers for random consistency index.

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

Table 2. Data security and privacy risk.

	Identity and access management risk	Multitenancy risk	Availability and backup risk	Weight of factor	Eigen value λ_{max}
Identity and access management risk	1	3	1/9	0.2782	7.2257
Multitenancy risk	1/3	1	7	0.3789	
Availability and backup risk	9	1/7	1	0.3429	

Table 3. Organizational risk.

	Organization changes management risk	Resours planing risk	Organizational security management risk	Weight of factor	Eigen value λ_{max}
Organization changes management risk	1	9	5	0.7020	3.3546
Resours planing risk	1/9	1	1/7	0.0556	
Organizational security management risk	1/5	7	1	0.2424	

Table 4. Technical risk.

	Portability risk	Application development risk	Interoperability standards risk	Weight of factor	Eigen value λ_{max}
Portability risk	1	1/5	3	0.3024	6.6386
Application development risk	5	1	1/9	0.3048	
Interoperability standards risk	1/3	9	1	0.3927	

Table 5. Compliance and audit risk.

	SLA rules abide risk	Security audit risk	Weight of factor	Eigen value λ_{max}
SLA rules abide risk	1	5	0.8333	2.9908
Security audit risk	1/5	1	0.3333	

Table 6. Physical security risk.

	Infrastructure control risk	Specific jurisdictions risk	Weight of factor	Eigen value λ_{max}
Infrastructure control risk	1	7	0.8750	2.1429
Specific jurisdictions risk	1/7	1	0.1250	

Table 7. Identity and access management risk.

	Unauthorised acces risk	Administrative acces risk	Weight of factor	Eigen value λ_{max}
Unauthorised acces risk	1	1/3	0.1750	0.49
Administrative access risk	3	1	0.5250	

Table 8. Multitenancy risk.

	Isolation between tenants risk	Virtual attacks realization risk	Leakage between tenants risk	Weight of factor	Eigen value λ_{max}
Isolation between tenants risk	1	7	1/7	0.3333	
Virtual attacks realization risk	1/7	1	5	0.3178	7.4632
Leakage between tenant risk	7	1/5	1	0.3489	

Table 9. Availability and backup risk.

	Service availability risk	Future operation risk	Backup related risk	Weight of factor	Eigen value λ_{max}
Service availability risk	1	4	6	0.6264	
Future operation risk	1/4	1	1/7	0.0933	4.0091
Backup related risk	1/6	7	1	0.2803	

Table 10. Organizational change management risk.

	Change people work risk	Resistance of change risk	Weight of factor	Eigen value λ_{max}
Change people work risk	1	3	0.7500	2
Resistance of change risk	1/3	1	0.2500	

Table 11. Portability risk.

	Hardware maintenance risk	Hardware failure risk	Weight of factor	Eigen value λ_{max}
Hardware maintenance risk	1	1/8	0.1111	1.9998
Hardware failure risk	8	1	0.8888	

Table 12. Application development risk.

	Technology and service failure risk	Resource sharing isolation risk	Weight of factor	Eigen value λ_{max}
Technology and service failure risk	1	2	0.6667	1.9910
Resource sharing isolation risk	1/2	1	0.3333	

Table 13. SLA rules abide risk.

	Illegal clauses risk	Jurisdiction abide risk	Weight of factor	Eigen value λ_{max}
Illegal clauses risk	1	4	0.8	2
Jurisdiction abide risk	1/4	1	0.2	

Table 14. Security audit risk.

	External audit risk	Security certification risk	Recovery method risk	Weight of factor	Eigen value λ_{max}
External audit risk	1	1	7	0.4940	
Security certification risk	1	1	1/4	0.2212	4.7362
Recovery method risk	1/7	4	1	0.2849	

Table 15. Infrastructure control risk.

	Staff training risk	Data center physical security risk	Weight of factor	Eigen value λ_{max}
Staff training risk	1	5	0.8333	2.9908
Data center physical security risk	1/5	1	0.3333	

Table 16. Specific jurisdictions risk.

	Specific jurisdiction location risk	Specific jurisdiction privacy risk	Weight of factor	Eigen value λ_{max}
Specific jurisdiction location risk	1	3	0.7500	2
Specific jurisdiction privacy risk	1/3	1	0.2500	

Table 17. Technological problem risk.

	Security and privacy risk	Organizational risk	Technical risk	Weight of factor	Eigen value λ_{max}
Security and privacy risk	1	6	2	0.5467	3.1589
Organizational risk	1/6	1	1/8	0.0700	
Technical risk	1/2	8	1	0.3833	

Table 18. Legal problem risk.

	Physical security risk	Compliance and audit risk	Weight of factor	Eigen value λ_{max}
Physical security risk	1	4	0.8	2
Compliance and audit risk	1/4	1	0.2	

Table 19. Cloud security level risk.

	Technological problem risk	Legal problem risk	Weight of factor	Eigen value λ_{max}
Technological problem risk	1	9	0.9	2
Legal problem risk	1/9	1	0.1	

Step 6. Calculation of consistency index (CI) and consistency ratio (CR).

$$\mathrm{CI} = \frac{\lambda_{\max} - n}{n-1} \tag{5}$$

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{6}$$

where, n is the number of factors, RI is random consistency index and is determined by Saaty as in **Table 1**.

Having obtained the risk priorities vector of cloud provider, we are able to calculate the risk value of cloud provider according to fuzzy logic of fuzzy set theory.

4. Fuzzy Risk Assessment

Fuzzy logic inference process for risk assessment can be described as a system which contain following blocks (**Figure 3**).

In this paper Mamdani type fuzzy logic inference algorithm is used. Mamdani type fuzzy logic inference model mainly contains the following five assessment steps:

Step 1. Fuzzification. In this step determination of main parameters which become necessary for risk assessment is performing. Due to uncertainty nature of these parameters their measurement are too complex. Therefore, the measure of each parameter is shown by linguistic terms and transforming to the appropriate fuzzy number.

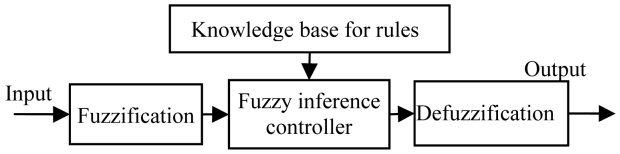

Figure 3. Procedures of fuzzy logic for cloud risk assessment.

In this study, we adopt triangular membership function. A triangular membership function is specified by three parameters $\{a,b,c\}$:

$$f(x;a,b,c)=\begin{cases}0, & x\le a\\ \dfrac{x-a}{b-a}, & a\le x\le b\\ \dfrac{c-x}{c-b}, & b\le x\le c\\ 0 & c\le x\end{cases} \tag{7}$$

By using the defined membership functions, we replace the input values with a set of linguistic values and assign a membership degree for each linguistic value using triangular membership functions.

Step 2. Construction of fuzzy rules. A fuzzy rule can be defined as a conditional statement in the form: "IF x is A THEN y is B" where x and y are linguistic variables and A and B are linguistic values determined by fuzzy sets on the universe of discourses X and Y, respectively. In this study, the fuzzy logic system is represented with three fuzzy sets low, medium, high. These fuzzy sets determine the shape and location of the membership functions.

Step 3. Inference. The inference engine makes decisions based on fuzzy rules. In other words, in this step calculation of output parameters for the rules are conducting here. For example, rule output parameter $B_i'(y)$ for the *i*-th rule " If x is A_i then y is B_i" is represented by following formula

$$B_i'(y)=\sup_{x\in X}\left(T\left(A'(x),T\left(A_i(x),B_i(y)\right)\right)\right) \tag{8}$$

where $A'(x)$ is the system input parameter, x is elements of the universal X set of input parameters of the system and y is elements of the universal Y set of output parameters of the system.

In this study, the inference engine for main block makes decisions based on 15 fuzzy inference rules as shown in **Figure 4**.

Step 4. Aggregation. Single output of rule knowledgebase are obtaining by aggregating of $B_i'(y)$ output parameters of all rules and calculating by the following formula

$$B_{out}'(y)=S\left(B_n'(y),S\left(B_{n-1}'(y),S\left(\cdots,S\left(B_2'(y),B_1'(y)\right)\right)\right)\right) \tag{9}$$

Step 5. Defuzzification. In this step, implementation of transformation of the linguistic value of cloud risk level into crisp risk values is carried out. We adopt the most common defuzzification method, called center of gravity to obtain the risk value of cloud provider with a value in the range $[0,1]$.

$$y_{out}=\int\frac{B_{out}'(y)z\mathrm{d}z}{B_{out}'(y)\mathrm{d}y} \tag{10}$$

5. Experiments on the Proposed Method

The proposed risk assessment system was built in the Matlab program in Fuzzy Inference Toolbox and Simulink environment.

First of all, decision-making matrixes are constructed by providing pairwise comparison within the AHP scale framework for the main factors and their sub factors as shown below and weight ratios were calculated for each factors (**Tables 2-19**).

Here 21 Mamdani-type decision-making subsystems are constructed. General fuzzy inference system for last main block of the general risk assessment system is illustrated in **Figure 5**.

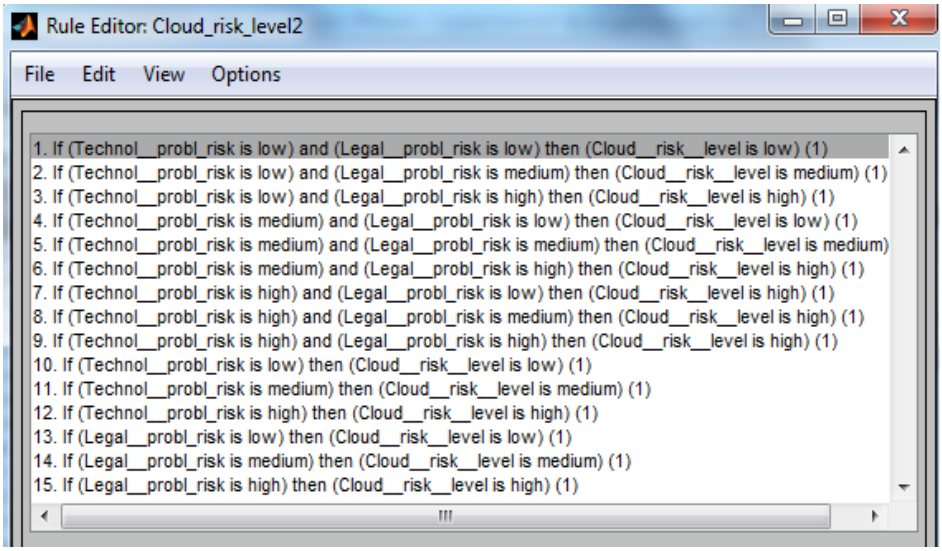

Figure 4. The fuzzy rulers defined for cloud security level risk subsystem.

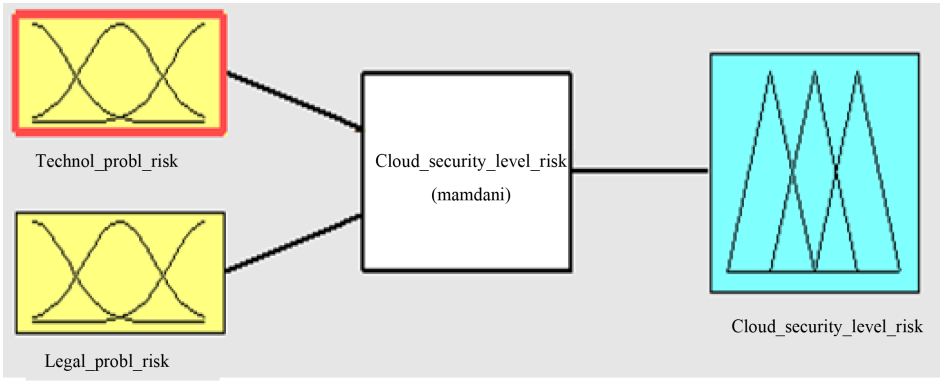

Figure 5. Fuzzy inference system for main risk factor.

In order to form a single risk assessment system all of the created subsystems are integrated. Simulink model was created in Matlab software environment for the demonstration of the capabilities of the proposed fuzzy approach for the risk assessment in the clouds (**Figure 6**).

The risk assessment is executed through the hierarchy from the bottom level to the highest multiplying each factor by its weight value.

In proposed model, the relevant input and output membership functions for each rule are shown in the following rule viewer window (**Figure 7**).

Here for the given input parameters the output membership function formed as a domain shown in a blue color shape. But in the bottom right area of the rule viewer window is illustrated the aggregated form of the membership functions. This represents the result of the fuzzification. Here, the center of gravity method is usedas a defuzzification method and in the bottom right area of the rule viewer window the red line represents the central point of the area, it represents the obtained output value of the risk assessment system. Here the input parameters added to the system with the linearly increasing number.

The units derived from the output signals of the system, shows that each factor can influence to the risk level of the clouds in a various forms. Final risk evaluation diagram of the system is illustrated in **Figure 8**. 3-dimensional surface model on both risk factor groups of risk assessment method is shown in **Figure 9**.

On the basis of proposed approach in a case the IdP (Identity Provider) and the SP (Service Provider) are unknown to each other, they can federate by estimating their risk level. And the decision to federation is making according to internal thresholds taken by the providers. In other words, on the basis of proposed collaborative

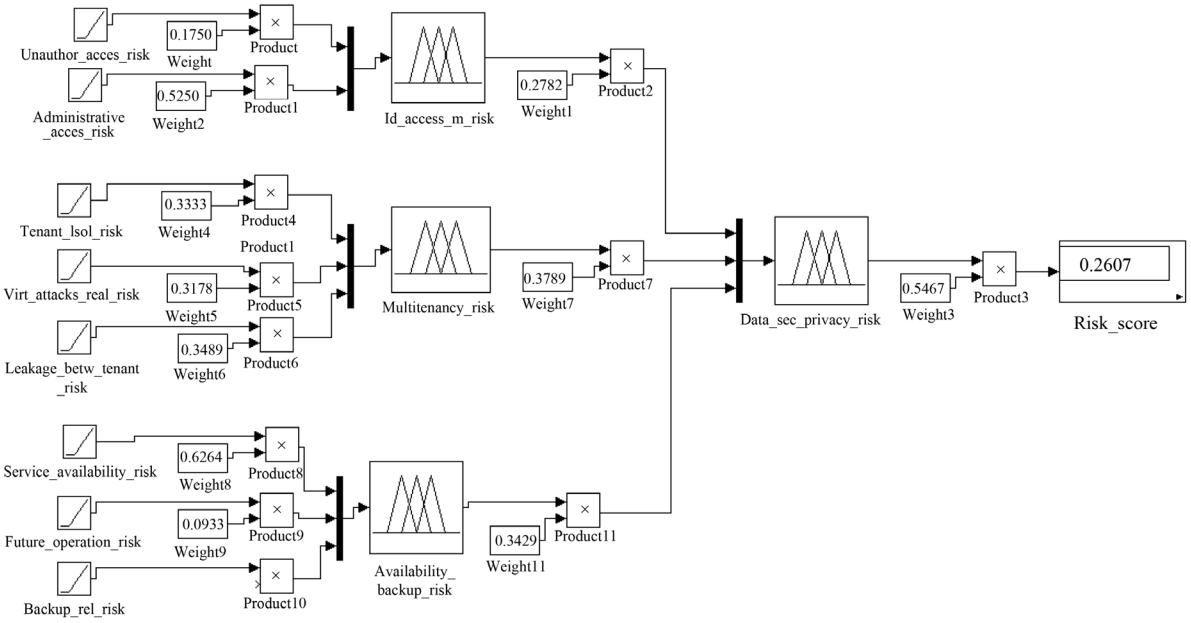

Figure 6. Cloud risk assessment model.

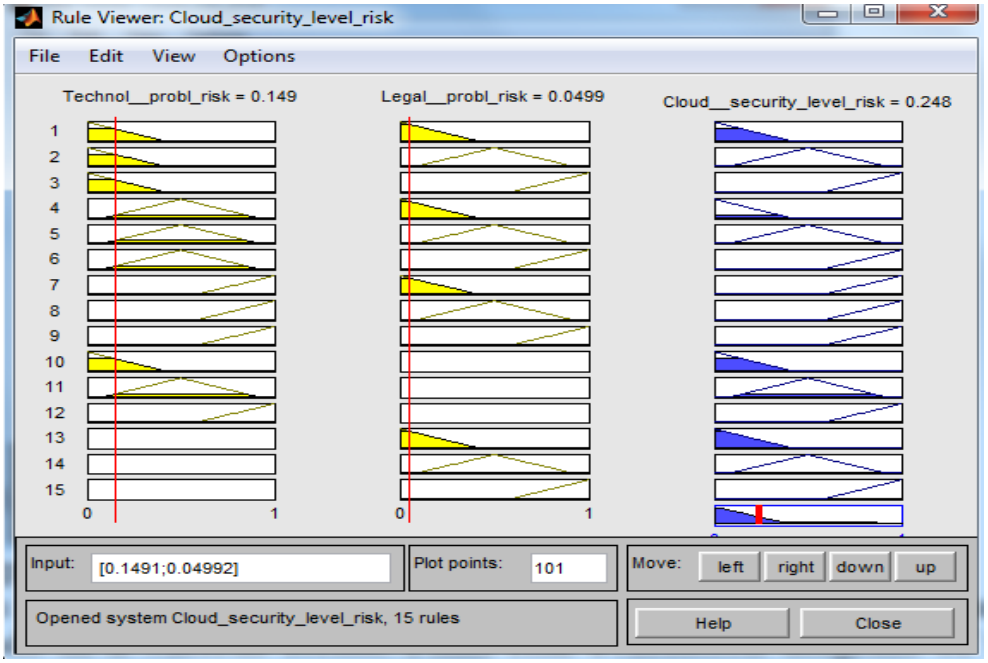

Figure 7. Input and output membership functions for each rule.

risk assessment method SP's risk value are calculating, and then obtained this risk value is comparing with the internal threshold of the IdP. If the final risk value is assumable according to internal thresholds, then they include each other to their own dynamic trust list, thus they are considered as federated.

6. Conclusions

Cloud technologies have led to a great revolutionary on the Internet since their emergence. But its series security problems have created a serious obstacle to prevalence of this technology. One of the main problems is the need

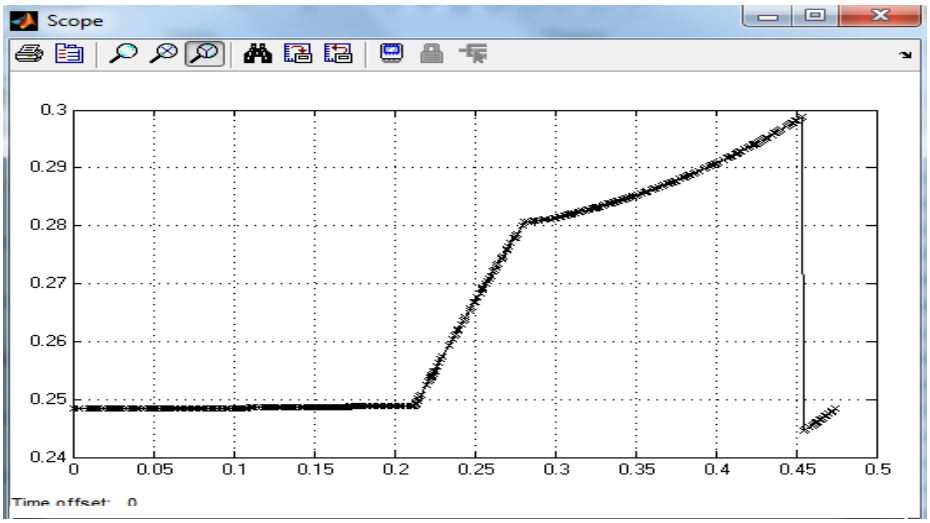

Figure 8. Influence of factors to the cloud risk level.

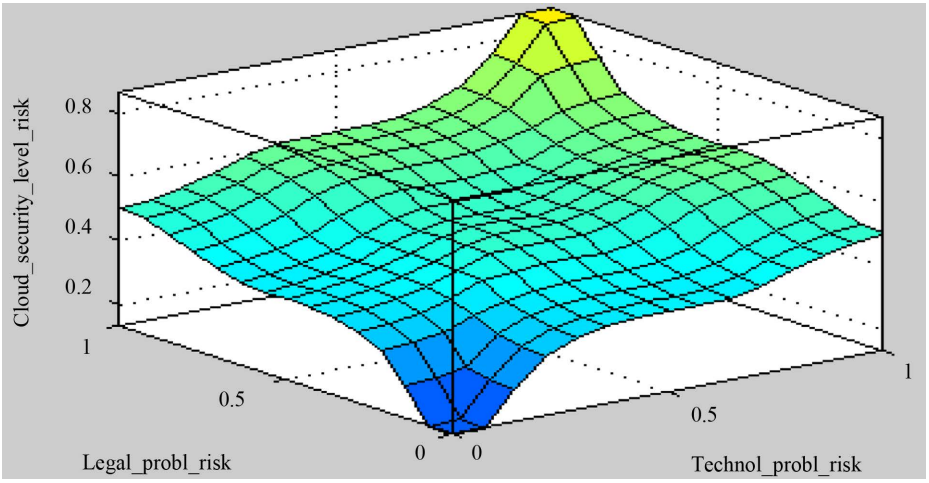

Figure 9. 3-d surface model based on both risk factor groups.

to create high-quality identification systems. Federative systems are used as identification systems in the clouds and they usually perform cloud federations through the identity. However, the main problem of the existing federative system is a requirement for pre-establishing of trust among the entities who wish to federate; this approach is not considered suitable for cloud environments dominated under the uncertainty. Therefore the need to develop methods that provide dynamic federation of multiple clouds still has not been met in the world science.

In this paper an approach for the providing of the dynamic federations of clouds is proposed. The approach is based on risk assessment technology and allows the use of cloud federations without the need of identity federations. Here for the solving of this problem, first of all important factors which are capable of seriously influencing of the information security level of clouds are selected and then based on these factors hierarchical risk assessment architecture is proposed. Then in the Simulink environment of Matlab program, a general model of the proposed architecture is constructed. The system parameters are described in the form of fuzzy sets. An experimental implementation of the proposed method is conducted on the cloud providers.

Future Work

In the future studies the complex toolbox can be developed for the proposed collaborative risk assessment method, and it can be used in risk assessment process of all kinds enterprises, which have necessity of hierarchical risk assessment.

Acknowledgements

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan—Grant No. EIF-2013-9(15)-46/16/1.

References

[1] Alguliev, R.M. and Abdullayeva, F.C. (2013) Identity Management Based Security Architecture of Cloud Computing on Multi-Agent Systems. *Proceedings of the Third International Conference on Innovative Computing Technology* (*INTECH*), London, 29-31 August 2013, 123-126. http://dx.doi.org/10.1109/INTECH.2013.6653643

[2] Əliquliyev, R.M. and Abdullayeva, F.C. (2013) Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi. *İnformasiya Texnologiyaları Problemləri*, **1**, 3-14.

[3] Carlini, E., Coppola, M., Dazzi, P., Ricci, L. and Righetti, G., (2012) Cloud Federations in Contrail. *Euro-Par* 2011: *Parallel Processing Workshops*, **7155**, 159-168.

[4] Rochwerger, B. (2009) The Reservoir Model and Architecture for Open Federated Cloud Computing. *IBM Journal of Research and Development*, **53**, 535-545. http://dx.doi.org/10.1147/JRD.2009.5429058

[5] Buyya, R., Broberg, J. and Goscinski, A. (2011) Cloud Computing: Principles and Paradigms. John Wiley & Sons Inc., Hoboken. http://dx.doi.org/10.1002/9780470940105

[6] Maler, E. and Reed, D. (2008) The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Security & Privacy*, **6**, 16-23. http://dx.doi.org/10.1109/MSP.2008.50

[7] Santos, D.R., Westphall, C.M. and Westphall, C.B. (2013) Risk-Based Dynamic Access Control for a Highly Scalable Cloud Federation. *Proceedings of the Seventh International Conference on Emerging Security Information*, *Systems and Technologies* (*SECURWARE* 2013), Barcelona, 25-31 August 2013, 8-13.

[8] Cabarcos, P.A. (2011) Risk Assessment for Better Identity Management in Pervasive Environments. *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops* (*PERCOM Workshops*), Seattle, 21-25 March 2011, 389-390. http://dx.doi.org/10.1109/PERCOMW.2011.5766913

[9] ETSI GS INS 004 (2010) Identity and Access Management for Networks and Services; Dynamic Federation Negotiation and Trust Management in IdM Systems.

[10] Cabarcos, P.A., Marín, A.L., Sánchez, R.G., Almenares, F.M. and Sánchez, D.D. (2012) A Metric-Based Approach to Assess Risk for on Cloud Federated Identity Management. *Journal of Network and Systems Management*, **20**, 513-533. http://dx.doi.org/10.1007/s10922-012-9244-2

[11] Cloud Security Aliance (CSA) https://cloudsecurityalliance.org

[12] ENISA (2009) Benefits, Risks and Recommendations for Information Security.

[13] Latif, R., Abbas, H., Assar, S. and Ali, Q. (2014) Cloud Computing Risk Assessment: A Systematic Literature Review. *Future Information Technology*. *Lecture Notes in Electrical Engineering*, **276**, 285-295. http://dx.doi.org/10.1007/978-3-642-40861-8_42

[14] Ammar, F.B., Hafsa, I.H. and Ouni, F. (2011) Analytic Hierarchical Process for Multicriteria Decision Making in design of Flying Voltage Source Multilevel Inverters. *European Journal of Electrical Engineering*, **14**, 719-756. http://dx.doi.org/10.3166/ejee.14.719-756

[15] Nataraj, S. (2005) Analytic Hierarchy Process as a Decision-Support System in the Petroleum Pipeline Industry. *Issues in Information Systems*, **VI**, 16-21.