UOT 004.056

Abdullayeva F.C.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
farqana@iit.ab.az

BULUDLARIN DİNAMİK FEDERALLAŞMASI ÜÇÜN MÜŞTƏRƏK RİSK QİYMƏTLƏNDİRİLMƏSİ ÜSULUNUN İŞLƏNMƏSİ

Məqalədə buludların dinamik federallaşmasına imkan verən yanaşma təklif edilir. Yanaşma risk qiymətləndirilməsi texnologiyasına əsaslanır və buludların federallaşmasını identifikasiyaların federallaşmasını nəzərə almadan həyata keçirir. Bu problemin həlli üçün ilk öncə buludların informasiya təhlükəsizliyi səviyyəsinə ciddi təsir edə bilən faktorların seçimi aparılır və bu faktorların əsasında iyerarxik risk qiymətləndirilməsi arxitekturu təklif edilir. Sonra analitik iyerarxiyalar prosesi (analytic hierarchy process, AHP) metodologiyası tətbiq olunaraq bulud provayderinin risk prioritetləri vektoru formalaşdırılır və bu vektorun əsasında qeyri-səlis məntiqi çıxarış tipli risk qiymətləndirilməsi aparılır.

Açar sözlər: *bulud texnologiyaları, federallaşma, risk qiymətləndirilməsi, çoxkirayəçilik.*

Giriş

Bulud texnologiyaları kimi geniş miqyaslı paylanmış sistemlərdə adətən müxtəlif subyektlər arasında qarşılıqlı əlaqələrin qurulması lazım gəlir [1, 2]. Əksər hallarda bu subyektlər müxtəlif təhlükəsizlik siyasətləri altında idarə olunan ayrı-ayrı şəbəkə domenlərinə məxsus olur. Burada qarşılıqlı əlaqələrin qurulmasına buludları federallaşdırmaqla (birləşdirməklə) nail olurlar [3, 4]. Federallaşma bulud texnologiyalarının əsas prinsiplərindən biridir [5].

Federallaşma sözü latın mənşəli *Foederatus* sözündən götürülmüşdür, *"müqavilə (foedus) əsasında birləşmiş tayfalar", "ittifaq" (allied)* mənasını verir. Bu terminin kökü qədim Roma dövrünə təsadüf edir. O dövrlərdə döyüşçülərdən ibarət tərkib yaratmaq məqsədi ilə Roma vətəndaşı olmayan şəxslərdən ibarət, müqavilə (*foedus*) əsasında tayfalar formalaşdırırdılar və bu tayfaların hər birini *Foederatus* adlandırırdılar və münaqişə yarandıqda onlardan silahlı qüvvə kimi istifadə edirdilər. Burada kənar millət nümayəndələrindən formalaşmış tayfa üzvlərini federatlar (federates), latınlardan ibarət formalaşdırdıqları tayfa üzvlərini isə "Qan müttəfiqləri" (blood allies) adlandırırdılar. *Foederatus* sözünün özü isə foedus (müqavilə (ing., treaty)) və fidere (inam (ing., trust) sözlərindən törənmişdir. Sonralar bu termin digər sahələrə nüfuz etməyə başladı və nəticədə dövlətlərin federallaşması, identifikasiyaların federallaşması, buludların federallaşması və s. kimi terminlərin meydana gəlməsinə səbəb oldu.

Buludların federallaşması (cloud federation) – resursları paylaşmaq məqsədilə müxtəlif buludlar arasında əlaqələrin təşkili prosesidir [6].

Dövlətlərin federallaşması (State federation) – dövlətlərin bir mərkəzi hakimiyyət altında idarə olunacağına zəmanət verən müqavilənin əsasında birləşməsi prosesidir [7].

İdentifikasiyaların federallaşması (Identity federation) – identifikasiyaların idarəetmə modellərindən biridir, istifadəçinin identifikasiyalarının müəyyən inam çevrəsi daxilində identifikasiya provayderləri və servis provayderləri arasında paylaşılmasına imkan yaradır [8].

"Merriam Webster Dictionary" ensiklopediyasında federallaşma termini xəbər kimi "iki və daha çox subyekti bir arada birləşdirmək" mənasında istifadə olunur.

Elmi-tədqiqat işlərində adətən buludların federallaşmasını identifikasiyaların federallaşması hesabına təmin edirlər. Bu yanaşma uğurlu hesab olunmur, çünki, identifikasiyaların federallaşmasının çox sayda problemləri vardır: inam müqavilələrinə zərurət, miqyasın məhdudluğu, informasiya təhlükəsizliyi, gizlilik, identifikasiya provayderinin aşkarlanmasında problem, interoperabellik [9, 10]. Bundan əlavə [11]-də müəlliflər iddia edir ki, identifikasiyaların federallaşması modellərinin (məsələn, Security Assertion Markup Language, SAML) inam çevrəsinin qurulması ilə bağlı da ciddi problemləri vardır.

Mövcud federallaşma texnologiyalarının bu problemləri onların bulud mühiti üçün istifadəsini qeyri-qənaətbəxş edir. Çünki bulud mühiti qeyri-müəyyənliyin hökm sürdüyü bir mühitdir. Burada həmçinin aralarında inam münasibətləri qurulmayan, bir-birinə naməlum olan iki subyektin də əlaqə qurmasına zərurət yarana bilir.

Bu problemi aradan qaldırmaq üçün bir sıra təlimatlarda ad-hoc dinamik federallaşmanın təmin edilməsi üçün metodların işlənməsinin zəruriliyi iddia olunur [12].

Adətən ad-hoc federallaşmanı tərəflərin infrastrukturunun risk səviyyəsini qiymətləndirməklə təmin edirlər. Bu məqsədlə [13]-də iddia olunur ki, risk metrikalarından istifadə olunması mövcud federallaşma sistemlərində inam çevrəsi problemini çox uğurla aradan qaldıra bilər və burada buludlarda identifikasiyaların federallaşmasında istifadə oluna bilən taksonomiya şəklində təşkil olunmuş metrikalar çoxluğu müəyyən edilmişdir. [10]-da buludların risk qiymətləndirməsi əsasında federallaşmasını təmin edən yanaşma verilir, lakin burada ümumi mənzərəni təsvir etməyə cəhd edirlər, mükəmməl hesablama modelinin qurulmasına cəhdlər müşahidə olunmur.

Təqdim olunan məqalədə buludların federallaşmasını təmin edən və identifikasiyaların federallaşmasına zərurət qoymayan, lakin ondan istifadə edə bilən yanaşma irəli sürülür. Yanaşma risklərin qiymətləndirilməsi texnologiyasına əsaslanır. Bunun üçün AHP və qeyri-səlis Mamdani alqoritminin sintezi əsasında risk qiymətləndirilməsi üsulu təklif edilir. Burada təklif edilən yanaşmanın mövcud metodlardan fərqi odur ki, burada buludların federallaşması identifikasiyaların federallaşması məsələsinə gətirilmir, birbaşa infrastruktur qiymətləndirilməsi əsasında həyata keçirilir.

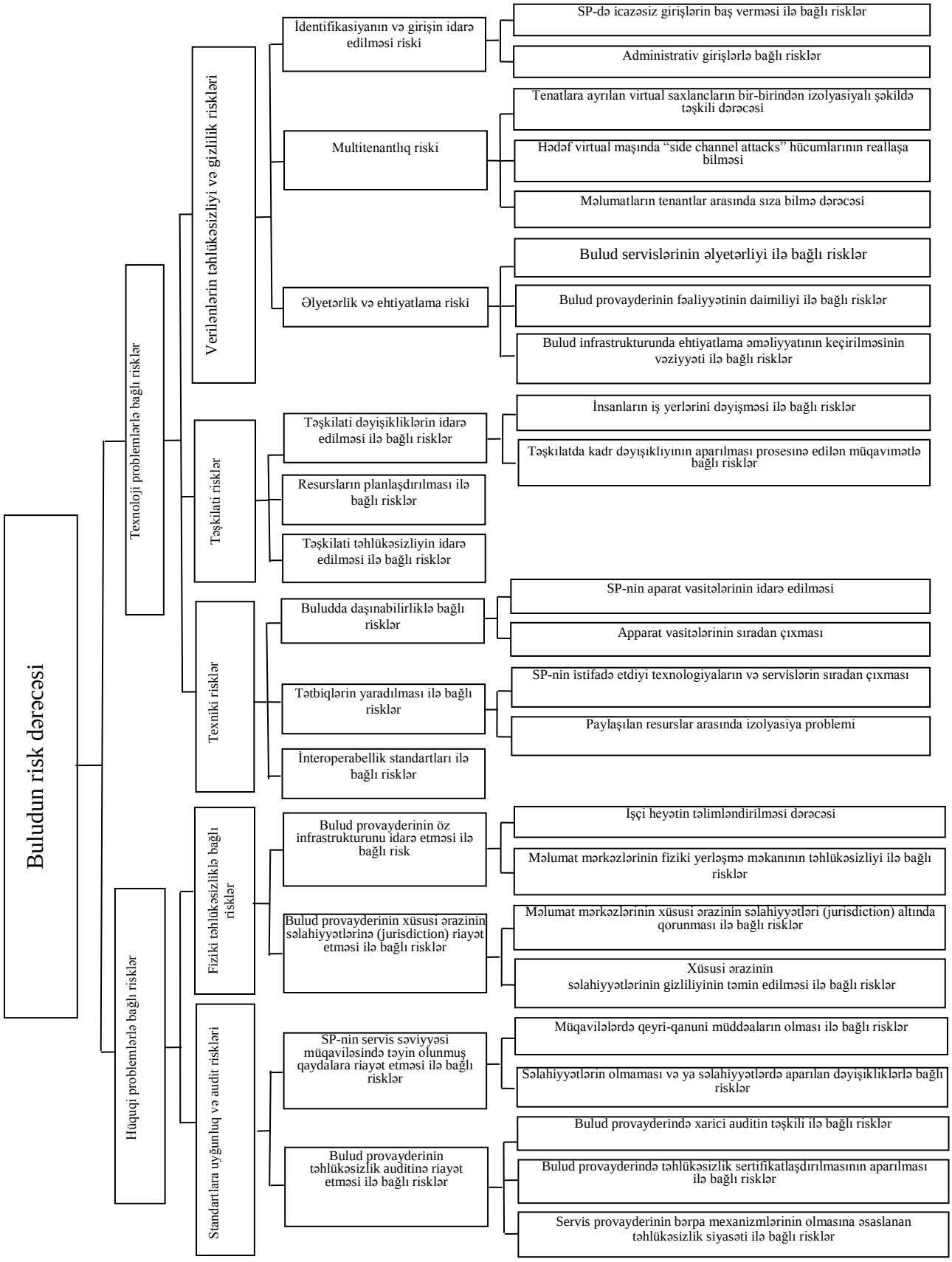
Tədqiqatın elmi ideyası

Buludların federallaşmasını təmin etmək üçün müxtəlif risk metrikalarından istifadə olunur. Kabarkos [13] buludlarda identifikasiyaların federallaşmasında istifadə oluna bilən taksonomiya şəklində təşkil olunmuş metrikalar çoxluğu müəyyən etmişdir. Lakin buludların federallaşması üçün yalnız identifikasiyaların federallaşması metrikaları kifayət qədər yetərli hesab olunmur [10]. Bunun üçün buludun infrastrukturunun təhlükəsizliyini pozmağa xidmət edən metrikaları da nəzərə almaq lazımdır. [14]-ə əsasən, buludun təhlükəsizlik səviyyəsinə ziyan vura bilən risk faktorları sırasına çoxkirayəçiliklə (multi-tenancy) bağlı riskləri, administrativ girişlərlə bağlı riskləri, provayderin xüsusi ərazinin səlahiyyətlərinə riayət etməsi ilə bağlı riskləri və s. aid etmək olar. Bütün bunları ümumiləşdirərək bulud provayderinin təhlükəsizliyinə böyük risk yarada bilən əsas faktorları verilənlərin təhlükəsizliyi və gizliliyi ilə bağlı risklər, təşkilati risklər, texniki risklər, standartlara uyğunluq və audit riskləri, fiziki təhlükəsizlik riskləri kimi klassifikasiya etmək olar.

Bu faktorları bir sıra aspektlərinə görə qruplaşdırmaq olar. Belə aspektlərdən biri faktorların hüquqi xarakter daşımasıdır, digəri isə texnoloji xarakter daşımasıdır. Bu yanaşmanı əsas götürərək buludların risk faktorlarını aşağıdakı şəkildəki kimi klassifikasiya etmək olar (şəkil 1).

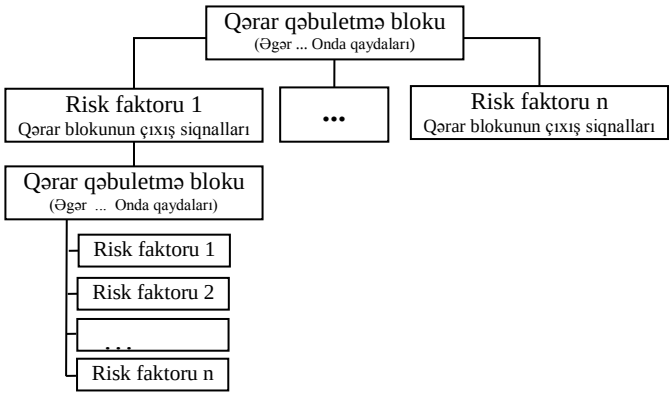
Belə klassifikasiya apardıqda sonuncu blok üçün iki giriş formalaşmış olur: buludların texnoloji problemləri ilə bağlı risklər və buludların hüquqi problemləri ilə bağlı risklər.

Burada ümumi risk qiymətləndirmə sistemi qərar qəbuletmə sistemiləri şəklində təşkil olunmuş ayrı-ayrı altsistemlərdən ibarət iyerarxik struktur şəklində təsvir edilmişdir. Bir altsistemin çıxışında alınan siqnallar növbəti qərar qəbuletmə sisteminin girişinə ötürülür. Bu ideyanı aşağıdakı şəkildəki kimi təsvir etmək olar (şəkil 2).



Şəkil 1. Buludda risk faktorlarının klassifikasiya sxemi

Beləliklə, bu komponentlər müxtəlif kriteriyalara görə birləşərək vahid bir risk qiymətləndirilməsi sistemi əmələ gətirir. Burada qərar qəbuletmə blokunun girişinə verilən giriş faktorları qeyri-səlis çoxluq şəklində, məsələn "aşağı, orta, yüksək" təsvir olunur. Burada qərar qəbuletmə sisteminin girişinə çəkili faktorlar daxil edilir, bu faktorlar üzərində çəkili qaydalar qurulur və alınmış nəticə çıxarış prosesinin növbəti mərhələsinə ötürülür. Qərar qəbuletmə sistemi "Əgər ... Onda" qaydaları əsasında təsvir olunur. Beləliklə, müştərək qərar qəbuletmə nəzəriyyəsinə əsaslanan bir risk qiymətləndirilməsi metodu təklif edilir.



Şəkil 2. İyerarxik risk qiymətləndirilməsi strukturu

Burada faktorların çəki əmsallarını müəyyən etməkdə məqsəd risk qiymətləndirilməsində dəqiqlik əldə etməkdir. Bunun üçün AHP metodundan istifadə edərək faktorlar üçün çəki əmsalları hesablanmışdır.

Analitik iyerarxiyalar prosesi metodu

Analitik iyerarxiyalar prosesi (Analytical Hierarchy Process, AHP) 1970-ci illərdə Tomas Saati tərəfindən yaradılmış konsepsiyadır. Müxtəlif tipli seçim kriteriyalarının iyerarxik şəkildə təşkili ideyasına əsaslanır. Bu metodologiya kriteriyaların bir-birinə nəzərən üstünlük dərəcəsini qiymətləndirməyə, alternativləri kriteriyalara görə müqayisə etməyə, namizədlərin ranqlanmasına, kriteriyaların çəkilərini müəyyən etməyə xidmət edir [15, 16].

AHP alqoritmi aşağıdakı kimi şərh olunur:

Addım 1. Qərar qəbulu iyerarxiyasının qurulması. Bizim tədqiqatda dörd təbəqəli iyerarxik struktur təklif edilmişdir (şəkil 1). İyerarxiyanın birinci təbəqəsini provayderin risk qiyməti təşkil edir. İyerarxiyanın 2-ci təbəqəsinə 2, 3-cü təbəqəsinə 5 faktor daxil edilmişdir: verilənlərin təhlükəsizliyi və gizlilik riskləri, təşkilati risklər, texniki risklər, standartlara uyğunluq və audit riskləri, fiziki təhlükəsizliklə bağlı risklər. İyerarxiyanın növbəti təbəqələrini bu faktorların altfaktorları təşkil edir.

Addım 2. Hər bir təbəqə üçün müqayisə matrisinin qurulması. Bu mərhələdə 9 ballıq sistemə əsasən faktorların bir-birinə nəzərən üstünlük dərəcələrini göstərən matris qurulur.

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

burada *i*-elementin yerləşdiyi sətrin, *j* isə sütunun nömrəsidir, a_{ij} - müqayisə matrisinin yuxarı diaqonal elementləri, $a_{ji} = \frac{1}{a_{ij}}$ - müqayisə matrisinin aşağı diaqonal elementləridir.

Addım 3. Normallaşdırılmış cüt-cüt müqayisə matrisinin qurulması. Normallaşdırılmış müqayisə matrisi A matrisinin hər bir elementini onun sütün elementləri cəminə bölməklə əldə olunur. *j* -cu sütunun elementləri cəmi $\sum_{i=1}^{n} a_{ij}$, $\forall i, j$ olduqda

$$a_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \qquad \forall i, j \tag{2}$$

Addım 4. Faktorlar üçün çəki qiymətlərinin hesablanması. Faktorların çəki qiymətləri normallaşdırılmış müqayisə matrisinin elementlərini sətir üzrə ortalamaqla əldə olunur. i-ci sətr üçün çəki əmsalı aşağıdakı kimi hesablanır:

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

burada n - faktorların sayıdır və təqdim olunan faktorlar üçün hasablanmış çəki əmsalları cədvəl 2−19-da göstərilmişdir.

Addım 4. Məxsusi qiymətin hesablanması. A qərar matrisinin məxsusi qiyməti çəki vektorunun hər bir elementini müqayisə matrisinin sütunları cəminə hasilləri ilə toplamaqla əldə olunur. Aşağıdakı düsturla hesablanır.

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

Addım 5. Uyğunluq indeksinin (consistency index, CI) və uyğunluq əmsalının (consistency ratio, CR) hesablanması.

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

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

Burada n - faktorların sayı, RI təsadüfi uyğunluq indeksidir (random consistency index) və Saati tərəfindən aşağıdakı cədvəldəki kimi təyin edilmişdir.

Cədvəl 1

Təsadüfi uyğunluq indeksinin qiymətləri

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

Beləliklə, yuxarıdakı AHP metodologiyası vasitəsilə bulud provayderinin *risk prioritetləri vektoru* formalaşdıqdan sonra, onun qeyri-səlis məntiqi çıxarış texnologiyası əsasında risk qiymətinin hesablanması aparılmalıdır.

Qeyri-səlis risk qiymətləndirilməsi

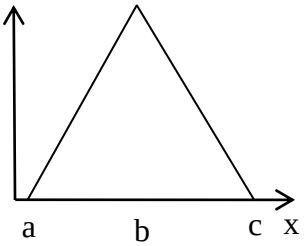
Riskin qiymətləndirilməsi üçün qeyri-səlis məntiqi çıxarış prosesi şəkil 3-də təsvir olunmuşdur.

Şəkil 3. Buludların risk qiymətləndirilməsi üçün qeyri-səlis məntiqi çıxarış prosesi

Təqdim olunan məqalədə Mamdani tipli qeyri-səlis məntiqi çıxarış alqoritmi istifadə olunmuşdur. Qeyri-səlis Mamdani çıxarış modelində qiymətləndirmə mərhələləri aşağıdakı addımlardan ibarətdir:

Addım 1. Fazifikasiya. Bu mərhələdə riskin qiymətləndirilməsi üçün lazım olan əsas parametrlərin təyin edilməsi həyata keçirilir. Bu parametrlər qeyri-müəyyənlik xüsusiyyətinə malik olduğu üçün onların ölçülməsi olduqca mürəkkəbdir. Bu səbəbdən hər bir parametrin ölçüləri linqvistik termlərlə göstərilir və uyğun qeyri-səlis ədədə çevrilir.

Təqdim olunan tədqiqat işində üçbucaq mənsubiyyət funksiyasından istifadə olunur (şəkil 4). Üçbucaq mənsubiyyət



Şəkil 4. Üçbucaq mənsubiyyət funksiyası

funksiyası 3 parametrlə $\{a, b, c\}$ təyin olunur və aşağıdakı kimi yazılır:

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

Göstərilən mənsubiyyət funksiyasından istifadə etməklə giriş qiymətləri linqvistik qiymətlərlə əvəz olunur və hər bir linqvistik qiymətə mənsubiyyət dərəcəsi mənimsədilir.

Addım 2. Qeyri-səlis qaydaların qurulması. Qeyri-səlis qayda aşağıdakı kimi göstərilmiş şərti mülahizə şəklində təyin olunur: "IF x is A THEN y is B", burada x və y linqvistik dəyişənlər, A və B isə qeyri-səlis çoxluqlarla təyin edilən linqvistik qiymətlərdir. Burada qeyri-səlis məntiqi çıxarış sistemi üç qeyri-səlis çoxluqla "aşağı", "orta", "yüksək" təsvir olunur. Bu qeyri-səlis çoxluqlar mənsubiyyət funksiyasının formasını və vəziyyətini müəyyən edir.

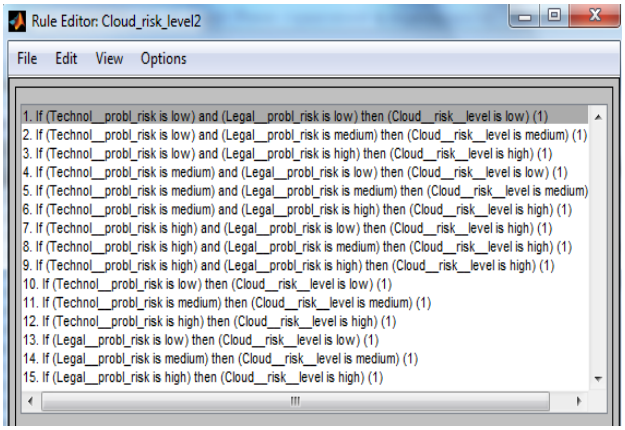
Addım 3. Çıxarış. Çıxarış blokunun funksiyası qeyri-səlis qaydalar əsasında qərarlar qəbul etməkdir. Başqa sözlə, bu mərhələdə qaydalar üçün çıxış parametrlərinin hesablanması aparılır. Məsələn, "*If* x *is* A_i *then* y *is* B_i" şəkildə verilmiş i-ci qaydanın $B_i'(y)$ çıxış parametri aşağıdakı düsturla verilir

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

burada $A'(x)$ sistemin giriş parametri, x sistemin giriş parametrlərinin universal X çoxluğunun elementidir, y isə sistemin çıxış parametrlərinin universal Y çoxluğunun elementidir.

Bu tədqiqat işində əsas blokun çıxarış sistemi, şəkil 5-dən göründüyü kimi, 15 qeyri-səlis qaydaya əsasən qərar qəbul edir.

Addım 4. Aqreqasiya. Qaydalardan ibarət biliklər bazasının vahid çıxışı bütün qaydaların $B_i'(y)$ çıxış parametrlərinin aqreqasiyası hesabına əldə olunur və aşağıdakı düsturla hesablanır.



Şəkil 5. Buludun risk dərəcəsi altsistemi üçün müəyyən olunmuş qeyri-səlis qaydalar

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

Addım 5. Defazifikasiya. Bu mərhələdə defazifikasiya metodu tətbiq olunmaqla qeyri-səlis ədədin tam ədədi qiymətə çevrilməsi həyata keçirilir. Bulud provayderinin $[0,1]$ intervalında risk qiymətini əldə etmək üçün defazifikasiya metodu olaraq ağırlıq mərkəzi metodu seçilmişdir və aşağıdakı kimi ifadə olunur

$$y_{out}=\int\frac{B'_{out}(y)\,zdz}{B'_{out}(y)\,dy} \qquad (10)$$

Təklif edilən metodun eksperimental yoxlanması

Təklif edilən risk qiymətləndirilməsi sistemi Matlab proqramının qeyri-səlis çıxarış sistemində və Simulink mühitində yaradılmışdır.

Bunun üçün ilk öncə əsas faktorların və bu faktorların altfaktorları üçün AHP şkalası çərçivəsində cüt-cüt müqayisə apararaq aşağıdakı kimi qərar qəbuletmə matrisləri qurulmuşdur (cədvəl 2–19) və hər bir faktor üçün çəki əmsalları müəyyən edilmişdir.

Cədvəl 2

Verilənlərin təhlükəsizliyi və gizlilik riski

	İdentifikasiyanın və girişin idarə edilməsi riski	Çoxkirayəçilik riski	Əlyetərlik və ehtiyatlama riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
İdentifikasiyanın və girişin idarə edilməsi riski	1	3	1/9	0.2782	7.2257
Çoxkirayəçilik riski	1/3	1	7	0.3789	
Əlyetərlik və ehtiyatlama riski	9	1/7	1	0.3429	

Cədvəl 3

Təşkilati risk

	Təşkilati dəyişikliklərin idarə edilməsi riski	Resurs planlaşdırma riski	Təşkilati təhlükəsizliyin idarə edilməsi riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Təşkilati dəyişikliklərin idarə edilməsi riski	1	9	5	0.7020	3.3546
Resurs planlaşdırma riski	1/9	1	1/7	0.0556	
Təşkilati təhlükəsizliyin idarə edilməsi riski	1/5	7	1	0.2424	

Cədvəl 4

Texniki risk

	Portabellik riski	Tətbiq yaradılması riski	İnteroperabellik standartlarının olmaması riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Portabellik riski	1	1/5	3	0.3024	6.6386
Tətbiq yaradılması riski	5	1	1/9	0.3048	
İnteroperabellik standartlarının olmaması riski	1/3	9	1	0.3927	

Cədvəl 5

Standartlara uyğunluq və audit riski

	Servis səviyyəsi müqaviləsi riski	Təhlükəsizlik auditinə riayət riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Servis səviyyəsi müqaviləsi riski	1	5	0.8333	2.9908
Təhlükəsizlik auditinə riayət riski	1/5	1	0.3333	

Cədvəl 6

Fiziki təhlükəsizlik riski

	Provayderin infrastrukturunun idarə edilməsi riski	Xüsusi ərazi səlahiyyətlərinə riayət riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Provayderin infrastrukturunun idarə edilməsi riski	1	7	0.8750	2.1429
Xüsusi ərazi səlahiyyətlərinə riayət riski	1/7	1	0.1250	

Cədvəl 7

İdentifikasiyanın və girişin idarə edilməsi riski

	İcazəsiz giriş riski	Administrativ giriş riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
İcazəsiz giriş riski	1	1/3	0.1750	0.49
Administrativ giriş riski	3	1	0.5250	

Cədvəl 8

Çoxkirayəçilik riski

	Kirayəçilər arasında izolyasiya riski	Virtual hücumların reallaşması riski	Kirayəçilər arasında sızma riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Kirayəçilər arasında izolyasiya riski	1	7	1/7	0.3333	7.4632
Virtual hücumların reallaşması riski	1/7	1	5	0.3178	
Kirayəçilər arasında sızma riski	7	1/5	1	0.3489	

Cədvəl 9

Əlyetərlik və ehtiyatlama riski

	Servisin əlçatanlıq riski	Provayderin daimi fəaliyyəti ilə bağlı risk	Ehtiyatlama riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Servisin əlçatanlıq riski	1	4	6	0.6264	4.0091
Provayderin daimi fəaliyyəti ilə bağlı risk	1/4	1	1/7	0.0933	
Ehtiyatlama riski	1/6	7	1	0.2803	

Cədvəl 10

Təşkilati dəyişikliyin idarə edilməsi riski

	Şəxsin iş yerini dəyişməsi ilə bağlı risk	Kadr dəyişikliklərinə müqavimət riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Şəxsin iş yerini dəyişməsi ilə bağlı risk	1	3	0.7500	2
Kadr dəyişikliklərinə müqavimət riski	1/3	1	0.2500	

Cədvəl 11

Buludda daşınabilirliklə bağlı risk

	Aparat vasitələrinin idarə edilməsi riski	Aparat vasitələrinin sıradan çıxma riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Aparat vasitələrinin idarə edilməsi riski	1	1/8	0.1111	1.9998
Aparat vasitələrinin sıradan çıxma riski	8	1	0.8888	

Cədvəl 12

Tətbiqlərin yaradılması ilə bağlı risk

	Texnologiyanın və servisin sıradan çıxması riski	Resurslar arasında izolyasiya riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Texnologiyanın və servisin sıradan çıxması riski	1	2	0.6667	1.9910
Resurslar arasında izolyasiya riski	1/2	1	0.3333	

Cədvəl 13

Servis səviyyəsi müqaviləsində qaydalara riayətlə bağlı risk

	Qeyri-qanuni müddəa riski	Səlahiyyətlərə riayət riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Qeyri-qanuni müddəa riski	1	4	0.8	2
Səlahiyyətlərə riayət riski	1/4	1	0.2	

Cədvəl 14

Təhlükəsizlik auditinə riayətlə bağlı risk

	Xarici audit riski	Təhlükəsizlik sertifikatlaşması riski	Bərpa mexanizmi riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Xarici audit riski	1	1	7	0.4940	4.7362
Təhlükəsizlik sertifikatlaşması riski	1	1	1/4	0.2212	
Bərpa mexanizmi riski	1/7	4	1	0.2849	

Cədvəl 15

İnfrastrukturun idarə edilməsi ilə bağlı risk

	İşçi heyətin təlimləndirilməsi riski	Məlumat mərkəzinin fiziki yerləşmə riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
İşçi heyətin təlimləndirilməsi riski	1	5	0.8333	2.9908
Məlumat mərkəzinin fiziki yerləşmə riski	1/5	1	0.3333	

Cədvəl 16

Xüsusi ərazinin səlahiyyətlərinə riayətlə bağlı risk

	Xüsusi ərazi səlahiyyətləri riski	Xüsusi ərazi səlahiyyətlərinin gizlilik riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Xüsusi ərazi səlahiyyətləri riski	1	3	0.7500	2
Xüsusi ərazi səlahiyyətlərinin gizlilik riski	1/3	1	0.2500	

Cədvəl 17

Texnoloji problemlərlə bağlı risk

	Təhlükəsizlik və gizlilik riski	Təşkilati risk	Texniki risk	Çəki əmsalları	Məxsusi qiymət λ_{max}
Təhlükəsizlik və gizlilik riski	1	6	2	0.5467	3.1589
Təşkilati risk	1/6	1	1/8	0.0700	
Texniki risk	1/2	8	1	0.3833	

Cədvəl 18

Hüquqi problemlərlə bağlı risk

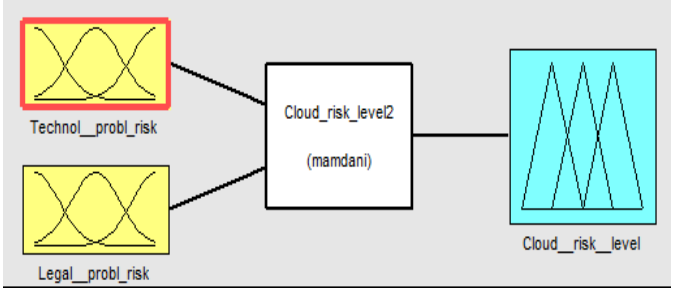
	Fiziki təhlükəsizlik riski	Standartlara uyğunluq riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Fiziki təhlükəsizlik riski	1	4	0.8	2
Standartlara uyğunluq riski	1/4	1	0.2	

Cədvəl 19

Buludun risk dərəcəsi

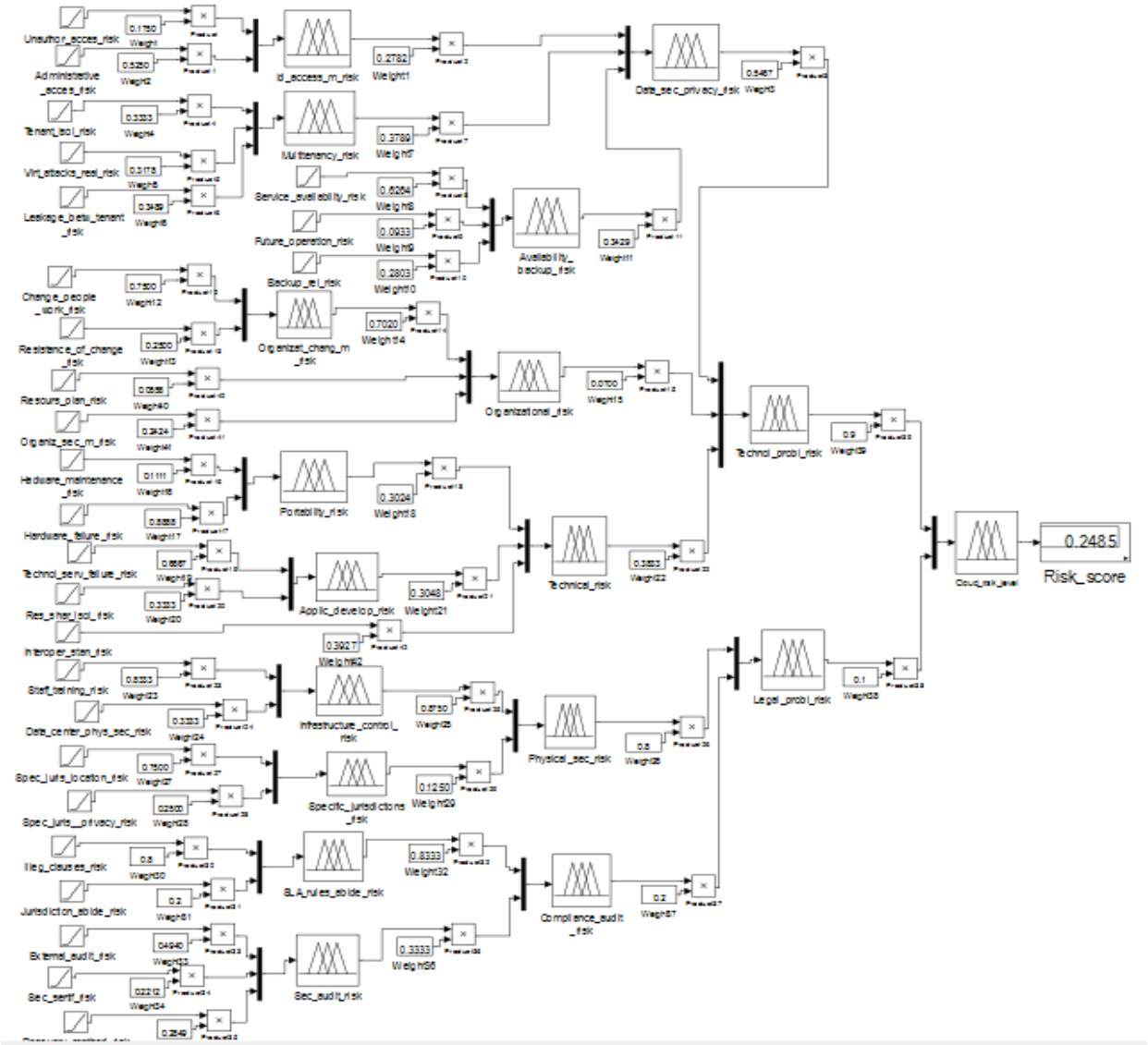
	Texnoloji problem riski	Hüquqi problem riski	Çəki əmsalları	Məxsusi qiymət λ_{max}
Texnoloji problem riski	1	9	0.9	2
Hüquqi problem riski	1/9	1	0.1	

Burada Mamdani tipli 21 qərar qəbuletmə altsistemləri qurulmuşdur. Ümumi risk qiymətləndirilməsi sisteminin sonuncu əsas bloku üçün qeyri-səlis qərar qəbuletmə sistemi şəkil 6-da əks etdirilir.



Şəkil 6. Əsas faktor üçün qeyri-səlis çıxarış sistemi

Burada vahid risk qiymətləndirilməsi sistemini formalaşdırmaq üçün yaradılmış altsistemlərin hamısı birləşdirilir. Buludlarda risk qiymətləndirilməsi üçün təklif edilən qeyri-səlis yanaşmanın imkanlarını nümayiş etdirmək üçün Matlab proqram mühitində onun Simulink modeli yaradılmışdır (şəkil 7).

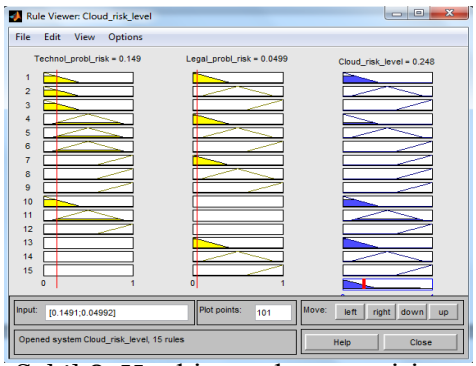


Şəkil 7. Buludun risk qiymətləndirilməsi modeli

Burada riskin qiymətləndirilməsi hər bir faktoru özünün çəki əmsalına vurmaqla iyerarxiyanın aşağı mərhələsindən başlayaraq yuxarıya doğru həyata keçirilməklə aparılır.

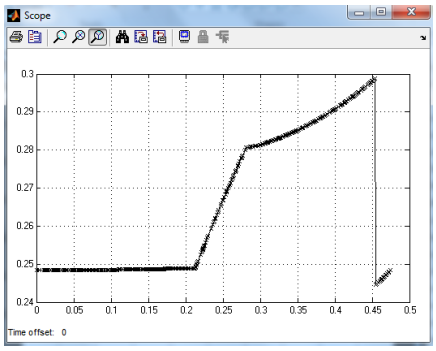
Təklif edilən modeldə hər bir qaydanın giriş və çıxış mənsubiyyət funksiyaları qaydalar pəncərəsində nümayiş etdirilir (şəkil 8).

Burada verilmiş giriş parametrləri üçün çıxış mənsubiyyət funksiyası mavi rənglərlə göstərilmiş oblastlar şəklində formalaşmışdır. Qaydalar pəncərəsinin sağ aşağı hissəsində isə mənsubiyyət funksiyalarının aqreqasiya olunmuş forması təsvir edilir. Bu fazifikasiyanın nəticəsini əks etdirir. Burada defazifikasiya üsulu olaraq ağırlıq mərkəzi metodundan (center of gravity) istifadə olunur və qaydalar pəncərəsinin sağ aşağı hissəsindəki mavi oblastda qırmızı xətt məhs elə sahənin mərkəzi nöqtəsini, yəni risk qiymətləndirilməsi sisteminin alınmış çıxış qiymətini əks etdirir. Burada sistemə giriş parametrləri xətti artan sıra ilə daxil edilir.



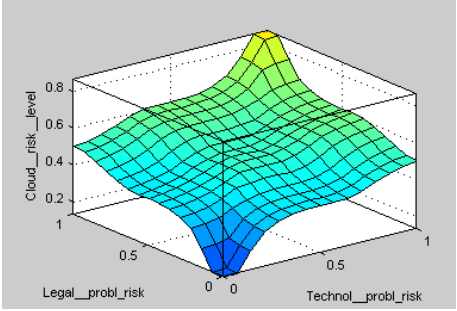
Şəkil 8. Hər bir qayda üçün giriş və çıxış mənsubiyyət funksiyaları

Bu sistemin çıxış siqnallarından alınan ədədlər göstərir ki, buludların risk dərəcəsinə hər bir faktor müxtəlif formada təsir edə bilir. Sistemin yekun risk qiymətləndirmə diaqramı şəkil 9-da təsvir edilir.



Şəkil 9. Faktorların buludun risk dərəcəsinə təsirini göstərən diaqram

Risk qiymətləndirilməsi üsulunun hər iki faktorlar qrupu üçün 3 ölçülü səth modeli şəkil 10-da təsvir edilir.



Şəkil 10. Risk faktorları qrupu üçün 3 ölcülü səth modeli

Təklif edilən yanaşmaya görə İdP (İdentifikasiya Provayderi) və SP (Servis Provayderi) bir-birinə naməlum tərəflər olduğu halda, onlar bir-birinin risk dərəcəsini qiymətləndirməklə federallaşa bilirlər. Federallaşmaq üçün qərar isə yalnız provayderin qəbul etdiyi daxili sərhəd qiyməti əsasında aparılır. Yəni təklif edilən müştərək risk qiymətləndirilməsi metodu əsasında SP-nin risk qiyməti hesablanır, sonra alınmış bu risk qiyməti İdP-nin daxili sərhəd qiyməti ilə müqayisə olunur. Əgər risk qiyməti qəbuledilməndirsə, onda onlar bir-birini özlərinin dinamik inam çevrəsinə daxil edir və bununla da federallaşmış hesab olunur.

Nəticə

Bulud texnologiyaları meydana gəldiyi dövrdən İnternet mühitində böyük inqilabi çevrilişə səbəb olmuşdur. Lakin onun silsilə təhlükəsizlik problemləri bu texnologiyanın geniş vüsət almasına ciddi maneə törədir. Burada başlıca problemlərdən biri yüksək keyfiyyətli identifikasiya sistemlərinin yaradılmasına ehtiyacın olmasıdır. Buludlarda identifikasiya sistemləri olaraq federativ sistemlərdən istifadə olunur və onlar buludların federallaşmasını adətən identifikasiyaların üzərindən həyata keçirir. Lakin mövcud federativ sistemlərin başlıca problemi, federallaşmaq istəyən tərəflər arasında əvvəlcədən inam münasibətlərinin qurulması tələbi olduğundan, bu yanaşma qeyri-müəyyənliyn hökm sürdüyü bulud mühitində əlverişli hesab olunmur. Bu səbəbdən ayrı-ayrı buludların dinamik federallaşmasını təmin edən metodların işlənməsi zərurəti hələ də öz həllini tapmamışdır.

Təqdim olunan məqalədə bir-birinə naməlum olan buludların dinamik federallaşmasına imkan verən yanaşma təklif edilir. Yanaşma risk qiymətləndirilməsi texnologiyasına əsaslanır və buludların federallaşmasını identifikasiyaların federallaşmasını nəzərə almadan həyata keçirir. Bu problemin həlli üçün ilk öncə buludların informasiya təhlükəsizliyi səviyyəsinə ciddi təsir edə bilən faktorların seçimi aparılır və bu faktorların əsasında iyerarxik risk qiymətləndirilməsi arxitekturu təklif edilir. Təklif edilən arxitekturanın Matlab proqramının Simulink mühitində ümumi modeli qurulmuşdur. Burada sistemin parametrləri qeyri-səlis çoxluqlar şəklində təsvir olunur. Təklif edilən metodun eksperimental tətbiqi bulud provayderləri üzərində aparılır.

Gələcək tədqiqatlar

Gələcək tədqiqatlarda buludlarda müştərək risk qiymətləndirilməsi üçün təklif edilən bu metod üçün kompleks bir proqram təminatı yaratmaq nəzərdə tutulur, onu iyerarxik risk qiymətləndirilməsinə ehtiyacı olan bütün növ müəssisələrin risk qiymətləndirilməsi prosesində də istifadə etmək olar.

Ədəbiyyat

1. Alguliev R.M., Abdullayeva F.C. Identity management based security architecture of cloud computing on multi-agent systems / Proc. of the third international conference on Innovative Computing Technology (INTECH), 2013, pp.123–126.
2. Əliquliyev R.M., Abdullayeva F.C. Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya Texnologiyaları Problemləri, 2013, №.1, s.3–14.
3. Carlini E., Coppola M., Dazzi P., Ricci L., Righetti G. Cloud Federations in Contrail / Proc. Euro-Par 2011: Parallel Processing Workshops, 2012, vol.7155, pp.159–168.
4. Rochwerger B. et al. The reservoir model and architecture for open federated cloud computing // IBM Journal of Research and Development, 2009, vol.53, no.4, pp. 535–545.
5. Buyya R., Broberg J., Goscinski A. Cloud Computing: Principles and Paradigms. John Wiley & Sons Inc., 2011, 637 p.
6. Kurze T., Klems M., Bermbach D., Lenk A., Tai S., Kunze M. Cloud Federation / Proc. of the second international conference on Cloud Computing, GRIDs, and Virtualization, 2011, pp.32–38.
7. Webster New World College Dictionary, http://www.yourdictionary.com/federation.
8. Lee H., Jeun I., Jung H. Criteria for evaluating the privacy protection level of identity management services / Proc. of the third international conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2009, pp.155–160.
9. Maler E., Reed D. The venn of identity: Options and issues in federated identity management // IEEE Security & Privacy, 2008, vol.6, no.2, pp.16–23.
10. Santos D.R., Westphall C.M., Westphall C.B. Risk based dynamic access control for a highly scalable cloud federation / Proc. of the seventh international conference on Emerging Security Information, Systems and Technologies (SECURWARE 2013), 2013, pp.8–13.
11. Cabarcos P.A. Risk assessment for better Identity Management in pervasive environments / Proc. of the IEEE international conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011, pp.389–390.
12. ETSI GS INS 004. Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems, 2010, 18 p.
13. Arias P.C., Marin A.L., Sanchez R.G., Almenares F.M., Sanchez D.D. A metric-based approach to assess risk for On cloud federated identity management // Journal of Network and Systems Management, 2012, vol.20, no.4, pp.513−533.
14. Latif R., Abbas H., Assar S., Ali Q. Cloud Computing Risk Assessment: A Systematic Literature Review // Future Information Technology, Lecture Notes in Electrical Engineering, 2014, vol.276, pp.285–295.
15. Ammar F.B., Hafsa I.H., Ouni F. Analytic Hierarchical Process for Multicriteria Decision Making in design of Flying Voltage Source Multilevel Inverters // European Journal of Electrical Engineering, 2011, vol.14, no.6, pp.719–756.
16. Nataraj S. Analytic Hierarchy Process as a Decision-Support System in the Petroleum Pipeline Industry // Issues in Information Systems, 2005, vol.VI, no.2, pp.. 16–21.

УДК 004.056
Абдуллаева Фаргана Д.
Институт Информационных Технологий НАНА, Баку, Азербайджан
farqana@iit.ab.az
Разработка совместного метода оценки риска для обеспечения динамической федерализации облаков
В статье предлагается подход для обеспечения динамической федерации облаков. Подход основан на технологии оценки рисков и позволяет обеспечить федерацию облаков без учета федерации идентификаций. Для решения этой проблемы, в первую очередь, отобраны важные факторы, которые способны существенно влиять на уровень информационной безопасности облаков, и на основе этих факторов предлагается иерархическая архитектура оценки степени риска. Затем, применяя методику АПИ (аналитический процесс иерархий), сформирован вектор приоритетов риска облачных провайдеров и, базируясь на нечеткой логике, осуществляется оценка рисков облачного провайдера.
Ключевые слова: *облачные вычисления, федерализация, оценка рисков, множественная аренда.*

Fargana C. Abdullayeva
Institute of Information Technology ANAS, Baku, Azerbaijan
farqana@iit.ab.az
Development of collaborative risk assessment method for dynamic federation of clouds
The article suggests an approach for the providing of the dynamic federation of clouds. An approach is based on risk assessment technology and allows the use of cloud federations without the need of identity federation. Here for the solving of this problem first of all an important factors which are capable of seriously influencing of the information security level of clouds are selected and then hierarchical risk assessment architecture is proposed based on these factors. Then by applying of the AHP methodology cloud provider's risk priority vectors are formed and on the basis of this vector fuzzy logic based risk value calculation is provided.
Keywords: *cloud computing, federation, risk assessment, multi-tenancy.*