

Bulud modellərinin təhlükəsizliyinin qeyri-səlis çoxkriteriyali qiymətləndirilməsi

Şəlalə Mansurova

AMEA İnformasiya Texnologiyaları İnstitutu

fmv.shalala@gmail.com

Xülasə—İnformasiya Kommunikasiya Texnologiyaları sahəsindəki inkişaf trendləri yüksək hesablama resursları tələb edən mürəkkəb məsələlərin həllində yeni texnologiyaların tətbiqini zərurətə çevirmişdir. Məqalədə yeni texnologiyaların praktik olaraq tətbiq edilməsi məqsədilə bulud texnologiyalarının təhlükəsizlik məsələlərinə baxılır, bulud hesablamalarındakı risklər və həlləri araşdırılır. Bulud modellərinin təhlükəsizlik baxımından çatışmazlıqları göstərilir.

Açar sözlər—hesablama buludları, bulud modelləri, bulud modellərinin təhlükəsizliyi, bulud xidmətləri

I. GİRİŞ

Hazırda bulud hesablamaları tədqiq edilən yeni bir istiqamətdir. Bulud hesablamaları paylanmış, dinamik olaraq miqyaslanı bilən paralel hesablama sistemidir. O, verilənlərin saxlanması və emalı kimi infrastruktur aktivlərindən istifadəyə, tətbiqlərə giriş əldə etməyə imkan verən əlaqələndirilmiş və virtuallaşdırılmış hesablama resursları toplusudur. Bulud texnologiyalarının tətbiqi yüksək emal göstəricilərinə nail olmağa imkan verir.

İstifadəçilərin buludlara İnternetə girişi olan istənilən qurğu vasitəsilə istənilən məkanda və istənilən zaman anında girişinin mümkünüyü bulud texnologiyalarının tətbiqini daha da genişləndirməyə şərait yaradan başlıca amillərdəndir. Lakin bu texnologiyanın tətbiqindəki əsas məsələ təhlükəsizlik problemlərinin mövcudluğu və onun idarə edilməsi üçün təhlükəsizlik siyasətinin olmamasıdır.

Bu məqsədlə məqalədə bulud hesablamalarının üzərinə qoyulan təhlükəsizlik tələbləri diqqətə çatdırılır. Müəyyən kriteriyalar üzrə bulud modellərinin təhlükəsizlik baxımından qiymətləndirilməsi həyata keçirilir. Qiymətləndirmə göstərilmiş kriteriyalar üzrə təhlükəsiz bulud modelini təyin etməyə imkan verir.

II. BULUD TEXNOLOGİYALARININ ANLAYIŞLARI

Bulud texnologiyalarının infrastrukturunu, kompüterlərin hesablama və yaddaş resurslarının klasterləşməsi və virtuallaşdırılmasından geniş istifadə etməklə, verilənlərin emalını və yadda saxlanmasını təmin edir [1]. Bulud texnologiyalarının köməyi ilə istifadəçilərin məlumatları bulud sistemlərində saxlanılır, emal edilir, emal proqramlarının işə salınması və nəticələrə baxılması təmin edilir.

Hər bir müəssisə, təşkilat təyinatından asılı olaraq

tətbiqlərin paylanması məqsədi ilə müxtəlif bulud növlərindən istifadə edə bilər. Buludların əsasən aşağıdakı modelləri fərqləndirilir:

Ümumi təyinatlı buludlar: Bu xidmətin istifadəçisi istənilən şirkət və istifadəçi ola bilər. Bu halda, bütün istifadəçilər məhdud konfigurasiyalı, mühafizə vasitəsilə təmin edilmiş eyni infrastrukturdan istifadə edir. Ümumi təyinatlı buludların üstün cəhətlərindən biri də onun təşkilatı buludlardan daha geniş miqyaslı olmasıdır. Buna görə də belə buludlar istifadəçilərin tələblərinə uyğun olaraq problemsiz şəkildə miqyaslanı bilər. Məsələn: Amazon EC2 və Simple Storage Service (S3), Google Apps/Docs, Salesforce.com, Microsoft Office Web onlayn xidmətlər ümumi istifadəli buludlara misal ola bilər.

Xüsusi təyinatlı buludlar: Yalnız bir təşkilat üçün istifadə və idarə edilir.

Hibrid buludlar: Bu növ buludlar ümumi və xüsusi təyinatlı bulud modellərinin kombinə edilməsi nəticəsində yaranmış modeldir. Hibrid buludlar bir sıra daxili və xarici bulud provayderləri tərəfindən istifadə olunan mühit kimi də başa düşülür.

Bulud hesablama arxitekturaları xidmət modellərinə əsasən aşağıdakı şəkildə təsnif edilir [2,3,6]:

Software as a Service (SaaS): Bu xidmət istifadəçilərə proqram təminatından istifadə etməyə imkan verir. Hazırda Google, Salesforce, Microsoft, Zoho və s. kimi şirkətlər tərəfindən bu səviyyədə istifadə edilən xidməti proqramlar təklif olunur.

Platform as a Service (PaaS): PaaS xidməti istifadəçilərə virtual serverlərdə yerləşən əməliyyat sistemlərindən və xüsusişədirilmiş proqram əlavələrindən istifadə edilməsinə imkan yaradır. Google App Engine, LAMP platform (Linux, Apache, MySQL and PHP), Force.com və s. PaaS xidmətlərinə misal ola bilər.

Infrastructure as a Service (IaaS): Bu xidmət istifadəçilərə kompüter infrastrukturundan istifadə etməyə imkan verir. IaaS xidmətinə misal olaraq Amazon S3 (Simple Storage Service), Amazon Elastic Computer Cloud (EC2), IBM Blue Cloud və s. qeyd etmək olar.

“İnformasiya təhlükəsizliyinin aktual problemləri”
III respublika elmi-praktiki seminarı, 08 dekabr 2017-ci il

III. BULUD HESABLAMALARININ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

Buludların tədqiqində ən böyük problemlərdən biri də onların təhlükəsizlik məsələləridir. Buludlar vasitəsilə verilənlərin virtual serverlərdə saxlanması və bunun kimi bir çox faktorlar bulud texnologiyalarının təhlükəsizliyinin təmin edilməsi məqsədilə müəyyən siyasət həyata keçirilməsini zərurətə çevirmişdir. Bu səbəbdən istifadəçilərdə buludların tətbiqi ilə bağlı tərəddüdlər yaranır. SaaS, PaaS və IaaS modellərinin təhlükəsizlik məsələlərinin həllinə yönəlmiş tədbirlər bilavasitə bulud sisteminin təhlükəsizliyinin təmin edilməsi tədbirlərinə adekvatdır[3,7]. Bu problemlərin tədqiqi ilə lazımı və adekvat təhlükəsizlik əldə edilə bilər. İnformasiya təhlükəsizliyinin mühüm aspektləri əlyətənlik, konfidensiallıq və bütövlüyün təmin edilməsi ilə həyata keçirilir. Bundan başqa etibarlılıq, idarəetmə, inteqrasiya kimi məsələlərə də baxılır.

Əlyətənlik dedikdə bulud istifadəçilərinin istənilən zaman anında və ixtiyari məkanda infrastruktura, tətbiqlər və verilənlərə girişinin olması nəzərdə tutulur. SaaS, PaaS və IaaS kimi bütün bulud hesablama sistemləri istifadəçilər üçün əlyətən olmalıdır. Təklif edilən xidmətlərin əlyətənliyi təhlükəsizliyə nəzarət strategiyaları ilə mühafizə edilə bilər. Misal olaraq IP adresə əsaslanan trafiklərin filterasiyası və blokladılması kimi üsulları qeyd etmək olar.

Bulud hesablamalarının istifadəsində üstünlüklər olduğu kimi onun bəzi çatışmayan cəhətləri də vardır:

- istifadəçilərin bulud xidməti göstərən şirkət və ya təşkilatlardan verilənlərinin asılılığı;
- bütün modellərdə təhlükəsizlik məsələlərinin eyni səviyyədə təşkil edilməməsi;
- bu sahədə keyfiyyətli xidmətə zəmanət verən metodlar və standartlar işlənməməsi və s.

IV. BULUD TƏHLÜKƏSİZLİYİNİN QIYMƏTLƏNDİRİLMƏSİ

Bulud texnologiyalarında qeyd olunan çatışmazlıqlar verilmiş məsələlərin həllinə tətbiqində ciddi maneə yaratmasa da, konkret modelin seçilməsində, təyin edilməsində diqqətə alınması vacib addım kimi tövsiyə olunur. Qiymətləndirmə buludlarda informasiya təhlükəsizliyi, idarəetməyə nəzarət, etibarlılıq, identifikasiya və avtorizasiya kimi xarakteristikalara əsasən həyata keçirilir [4,5]. Bu məqsədlə X_1 =" Xüsusi təyinatlı buludlar", X_2 ="Ümumi təyinatlı buludlar", X_3 ="Hibrid buludlar" alternativlərinin təhlükəsizlik baxımından seçilməsi zamanı daha adekvat buludun təyin edilməsi üçün aşağıdakı kriteriyalardan istifadə etmək olar:

- Information security;
- Authentication and Authorization;
- Control of governance;
- Reliability.

Verilmiş kriteriyaların hər birinin fazifikasiya cədvəli aşağıdakı kimidir:

CƏDVƏL 1. “INFORMATION SECURITY (K₁)” KRİTERİYASININ FAZİFİKASIYASI

Linqvistik dəyişən	Linqvistik qiymət	[0;1] interval
Yüksək təhlükəsizlik	Çox yaxşı	[0.9; 1]
Təhlükəsiz	Yaxşı	[0.7; 0.9]
Qismən təhlükəsiz	Orta	[0.5; 0.7]
Aşağı təhlükəsiz	Zəif	[0.1; 0.5]
Təhlükəsizlik təmin olunmur	Pis	[0; 0.1]

CƏDVƏL 2. “AUTHENTICATION AND AUTHORIZATION (K₂)” KRİTERİYASININ FAZİFİKASIYASI

Linqvistik dəyişən	Linqvistik qiymət	[0;1] interval
Yüksək identifikasiya olunma	Çox yaxşı	[0.9; 1]
Yaxşı identifikasiya olunma	Yaxşı	[0.7; 0.9]
Qismən yaxşı identifikasiya olunma	Orta	[0.5; 0.7]
Aşağı identifikasiya olunma	Zəif	[0.1; 0.5]
Zəif identifikasiya olunma	Pis	[0; 0.1]

CƏDVƏL 3. “CONTROL OF GOVERNANCE (K₃)” KRİTERİYASININ FAZİFİKASIYASI

Linqvistik dəyişən	Linqvistik qiymət	[0;1] interval
Yüksək idarəetmə səviyyəsi	Çox yaxşı	[0.9; 1]
Yaxşı idarəetmə	Yaxşı	[0.7; 0.9]
Qismən yaxşı idarəetmə	Orta	[0.5; 0.7]
Aşağı idarəetmə	Zəif	[0.1; 0.5]
Zəif idarəetmə	Pis	[0; 0.1]

CƏDVƏL 4. “RELIABILITY (K₄)” KRİTERİYASININ FAZİFİKASIYASI

Linqvistik dəyişən	Linqvistik qiymət	[0;1] interval
Yüksək etibarlılıq	Çox yaxşı	[0.9; 1]
Yaxşı etibarlılıq	Yaxşı	[0.7; 0.9]
Qismən etibarlıdır	Orta	[0.5; 0.7]
Aşağı etibarlılıq	Zəif	[0.1; 0.5]
Etibarlılıq təmin olunmur	Pis	[0; 0.1]

Hər bir bulud cədvəl 5 və cədvəl 6-dakı kimi verilmiş kriteriyalar əsasında öncə linqvistik qiymətlərlə, daha sonra linqvistik qiymətlərə uyğun olaraq [0;1] intervalından təyin edilmiş ədədlərlə qiymətləndirilir:

CƏDVƏL 5. KRİTERİYALAR ƏSASINDA BULUDLARIN LINQVİSTİK QIYMƏTLƏNDİRİLMƏSİ

	K1	K2	K3	K4
X1	Yaxşı	Əla	Əla	Orta
X2	Orta	Yaxşı	Orta	Yaxşı
X3	Əla	Yaxşı	Yaxşı	Orta

CƏDVƏL 6. KRİTERİYALAR ƏSASINDA BULUDLARIN ƏDƏDİ QIYMƏTLƏNDİRİLMƏSİ

	K1	K2	K3	K4
X1	0.75	0.91	0.95	0.52
X2	0.56	0.79	0.68	0.78
X3	0.91	0.82	0.78	0.68

“İnformasiya təhlükəsizliyinin aktual problemləri”
III respublika elmi-praktiki seminarı, 08 dekabr 2017-ci il

Ekspertlərdən tələb olunur ki, kriteriyalara vaciblik əmsalı təyin etmək üçün 0-9 şkalası üzrə hər bir kriteriyayı qiymətləndirsin. Qiymətləndirmənin nəticəsi cədvəl 7-də verilmişdir:

CƏDVƏL 7. KRİTERİYALARIN QIYMƏTLƏNDİRİLMƏSİ

	K1	K2	K3	K4	
E1	9	8	8	6	31
E2	7	9	6	8	30
E3	7	9	9	8	33
$\sum_{j=1}^3 k_j$	23	26	23	22	94

Baxılan məsələdə 3 ekspert rəyinə əsasən kriteriyalara vaciblik əmsalı (çəki) təyin edilir. Bunun üçün aşağıdakı düsturdan istifadə edilməklə cədvəl 8-dəki hesablamalar aparılır:

$$W_{k_{ij}} = \frac{\sum_{j=1}^m k_j}{\sum_{i=1}^n \sum_{j=1}^m k_{ij}} \quad (1)$$

Burada $W_{k_{ij}}$ kriteriyanın vaciblik əmsalı, k_j isə ekspertlərin kriteriyalara təyin edildikləri qiymətlərdir.

CƏDVƏL 8. KRİTERİYALARIN ÇƏKİ ƏMSALININ HESABLANMASI

Kriteriyalar	Kriteriyanın çəkisi
K_1	$W_{K1} = 23/94=0,24$
K_2	$W_{K2} = 26/94=0,27$
K_3	$W_{K3} = 23/94=0,24$
K_4	$W_{K4} = 22/94=0,23$

Multiplikativ aqreqatlaşma metodundan istifadə etməklə alternativlər qiymətləndirilir. Bu qiymətləndirmə aşağıdakı düstur vasitəsi ilə həyata keçirilir:

$$\varphi_k(X_i) = \prod_{j=1}^m \varphi_{kj}(X_i)^{w_j} \quad (2)$$

$$\varphi_k(X_1) = 0,75^{0,24} \cdot 0,91^{0,27} \cdot 0,95^{0,24} \cdot 0,52^{0,23} = 0,76$$

$$\varphi_k(X_2) = 0,56^{0,24} \cdot 0,79^{0,27} \cdot 0,68^{0,24} \cdot 0,78^{0,23} = 0,69$$

$$\varphi_k(X_3) = 0,91^{0,24} \cdot 0,82^{0,27} \cdot 0,678^{0,24} \cdot 0,68^{0,23} = 0,77$$

$$X_3 > X_1 > X_2$$

Cədvəl 9-dan göründüyü kimi baxılan məsələdə ən yaxşı seçim X_3 alternatividir.

CƏDVƏL 9. MULTIPLİKATİV METOD ƏSASINDA BULUD MODELİNİN QIYMƏTLƏNDİRİLMƏSİ

Alternativlər	Multiplikativ metod
$X_1 = Xüsusi təyinatlı buludlar$	0.76
$X_2 = Ümumi təyinatlı buludlar$	0.69
$X_3 = Hibrid buludlar$	0.77

NƏTİCƏ

Bulud texnologiyaları araşdırılmış və təyinatına görə bulud modellərinin təhlükəsizliyi, mövcud risklər təhlil edilmiş və bulud təhlükəsizliyinin qiymətləndirilməsi parametrləri müəyyən edilmişdir. Araşdırmalar onu göstərdi ki, bulud texnologiyalarının istifadəsi zamanı bulud xidməti infrastrukturunun, bulud modellərinin təhlükəsizlik baxımından üstün və çatışmayan göstəriciləri nəzərə alınmaqla mürəkkəb məsələlərin həlli üçün tətbiq edilə bilər. Bu faktorların nəzərə alınması ilə nəticə olaraq xərclərin azalmasını, yüksək emal göstəricilərini əldə etmək mümkündür.

ƏDƏBİYYAT

- [1] “Security recommendations for cloud computing providers”, White paper, 2012, 71p.
- [2] T. Mather, S. Kumaraswamy and S. Latif, “Cloud security and privacy”, First Edition, 2009, 335p.
- [3] S. Jafarpour and A. Yousefi, “Security risks in cloud computing: a review”, “International Journal of Current Engineering and Technology”, 2016, Vol.6, No.4, pp.2-6
- [4] A. Asma, M.A. Chaurasia and H.Mokhtar, “Cloud computing security issues”, “International Journal of Application or Innovation in Engineering & Management”, 2012, Vol.1, No.2, pp.3-5
- [5] A. Gupta, R. Thakur, G. Deol, “Cloud security and privacy”, “International Journal of Information and Technology (IJIT)”, 2016, Vol.2, No.3, pp.2-5
- [6] R.Q. Ələkbərov, M.A. Həşimov, T. İ. Mustafayev, “Cloud computing xidmətinin təhlükəsizlik məsələləri və onların həlli yolları”, “İnformasiya Texnologiyaları İnstitutu”, 2014, №2, s.33-39
- [7] R.M. Əliquliyev, F.C. Abdullayeva, “Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi”, “İnformasiya Texnologiyaları İnstitutu”, 2013, №1(7), s.3-14

FUZZY MULTI-CRITERIA EVALUATION OF CLOUD

MODELS SECURITY

Shalala Mansurova
Institute of Information Technology of ANAS, Baku, Azerbaijan
fmv.shalala@gmail.com

Abstract – The development trends in ICT made it necessary to use new technologies to solve complex problems that require high computational resources. In the article, the security issues of cloud technology for practical application of the new technology are considered, the risks and solutions of cloud computing are explored. The lack of security in cloud models is reviewed.

Keywords – cloud computing, cloud models, cloud models security, cloud services