

UOT 004.75

Ələkbərov R.Q.¹, Həşimov M.A.², Mustafayev T.İ.³

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹rashid@iit.ab.az, ²mhashimov@iit.ab.az, ³tural.mustafayev@iit.ab.az

CLOUD COMPUTİNG XİDMƏTİNİN TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ VƏ ONLARIN HƏLLİ YOLLARI

Məqalədə cloud computing texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması prinsipləri müəyyən edilmiş, AzScienceNet şəbəkəsində bulud və virtual resurslardan istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.

Açar sözlər: cloud computing, yaddaş və hesablama resursları, hesablama servisləri, cloud computing xidmətlərinin təhlükəsizliyi.

Giriş

Cloud computing – istifadəçiyə xidmət şəklində İnternet və ya lokal şəbəkə vasitəsilə əlyətərli olan proqram-aparat təminatıdır. Cloud computing müəyyən resurslara (hesablama resurslarına, proqram və məlumatlara) uzaq məsafədən müraciət etmək üçün rahat interfeysdən istifadə etməyə imkan verir. İstifadəçi kompüter, bu halda, şəbəkəyə qoşulmuş adi terminal rolunu oynayır [1].

Cloud computingdən xidmət kimi istifadə edilməsi haqqında ilk fikirlər 1960-cı illərdə informasiya texnologiyaları sahəsində şöhrətli alim olan Lisp dilinin ixtiraçısı, MTİ (Massachusetts Texnologiya İnstitutu) və Stanford Universitetinin professoru Con Makkarti (John McCarthy) tərəfindən irəli sürülmüşdür. İlk real layihə 1999-cu ildə qurulan Salesforce.com şirkəti tərəfindən həyata keçirilmişdir. Məhz o zaman "Proqram təminatı kimi Servis" ("SaaS") ifadəsi yaranmışdı. Salesforce şirkətinin cloud computing sahəsindəki uğuru İT sənayesinin nəhəng şirkətlərində maraq doğurmağa başladı və onlar cloud computing sahəsində tədqiqat apardıqları barədə məlumat yaydılar [1].

Hal-hazırda hesablama resursları su, işıq, qaz və telefon kimi ənənəvi kommunal xidmətlərindən ibarət modelə çevrilmişdir. Belə bir modeldə istifadəçilər xidmətlərin harada və ya necə həyata keçirildiyindən asılı olmayaraq, onların tələblərinə əsaslanan xidmətlərdən faydalanırlar. Müasir cəmiyyətin inkişafı ilə əsas kommunal xidmətlər, ümumilikdə elə təmin olunur ki, hər kəs onlardan asanlıqla faydalanmaq imkanı əldə edə bilsin. Bu gün su, elektrik enerjisi, qaz və telefon kimi kommunal xidmətlərin təmin edilməsi gündəlik həyat üçün zəruri hesab olunur. Bu kommunal xidmətlərə tələbat çox olduğuna görə onlar istənilən zaman əlyətərli olmalıdır. 1969-cu ildə Advanced Research Projects Agency Network (ARPANET) layihəsinin tanınmış alimlərindən və İnternetin yaradıcılarından biri olan Leonard Kleynrok söyləmişdir [2]: “Bu gün kompüter şəbəkələri hələ özünün “uşaqlıq” dövrünü yaşayır, böyüdükdən və yetkinləşdikdən sonra isə çox güman ki, onların da elektrik və telefon kimi kommunal xidmətə çevrilərək fərdi evləri və ya ofisləri təmin edəcəyini görəcəyik. Bu cür xidmət modelinə əsaslanmış hesablama kommunal xidməti 21-ci əsrin bütün kompüter sənayesinin kütləvi transformasiyasından xəbər verir.” Eynilə, kompüter istifadəçiləri (istehlakçıları) da kompüter xidmətlərindən istifadəyə görə provayderlərə ödənişlər etməlidirlər. Bundan əlavə, artıq istehlakçıların böyük sərmayə qoymağına və ya mürəkkəb IT infrastrukturunu yaratmasına ehtiyac qalmayacaq. “Bulud” hesablamaları konsepsiyası boş yerə meydana çıxmamış, son bir neçə onillik ərzində informasiya texnologiyalarının təkamül inkişafının nəticəsi və müasir biznes çağırışlarına cavab olaraq yaranmışdır. Gartner Group analitikləri informasiya texnologiyalarının bir çox hissəsinin 5–7 il ərzində “bulud” texnologiyalarına keçiriləcəyini proqnozlaşdıraraq, onu

gələcəyin ən perspektivli strateji texnologiyası adlandırırlar. Onların qiymətləndirməsinə görə, 2015-ci ilə bulud hesablamaları bazarının həcmi 200 milyard dollara çatdırılacaq [1].

Böyük hesablama və yaddaş resursları tələb edən mürəkkəb məsələlərin həllində son zamanlar cloud computing texnologiyalarından geniş istifadə edilir. Bu texnologiyaların üstünlüklərini nəzərə alaraq hal-hazırda AzScienceNet şəbəkəsi üzərində cloud computing xidmətinin istifadəsinə başlanmışdır. Bu xidmətin əsas məqsədi AMEA-nın institut və təşkilatlarında fəaliyyət göstərən tədqiqatçıların, AzScienceNet Data mərkəzinin böyük hesablama və yaddaş resurslarından istifadə edərək öz mürəkkəb məsələlərinin həllində istifadə etməsidir və bu resurslardan istifadə zamanı bir sıra təhlükəsizlik məsələləri ön plana çıxır.

Təqdim olunan işdə cloud computingdən istifadə zamanı istifadəçilərin məlumatlarının etibarlılığını təmin etmək üçün, *DDoS və buna bənzər hücumlar, parolun yığılma metodları ilə ələ keçirilməsi riski, konfidensial məlumatların 3-cü şəxslər tərəfindən mənimlənməsi təhlükəsi, fiziki serverlərin oğurlanması və ya sınıması halları, məlumatların itməsi təhlükəsi və qəza hallarından sonra bərpa, rabitə kanalı ilə ötürülən məlumatların digər şəxs tərəfindən tutulması* kimi təhlükəsizlik məsələlərinin həlli yolları analiz edilmişdir.

Cloud computing texnologiyalarının xidmətləri

Cloud computing istifadəçilərə 10-dan artıq xidmət təklif edir. Ən çox istifadə olunan xidmətlər aşağıdakılardır [4].

- *Infrastructure-as-a-service (IaaS) – infrastruktur xidməti kimi.*

IaaS xidməti infrastrukturun (hesablama və yaddaş sistemi) icarəyə götürülməsi servisini həyata keçirtməyə imkan verir. Bu resurslara zəmanətli hesablama və yaddaş resursları verən virtual serverlərdən başqa, verilənlərin yaddaş sisteminə yüksək sürətlə daxil edilməsi imkanı yaradan əlaqə kanalları da daxildir. Qısaca desək, bu səviyyədə məsələlərin həlli üçün kompüter infrastrukturunu yaradılır. Mövcud olan IaaS xidmətlərinə - Amazon S3, Amazon Elastic Computer(EC2), IBM Blue Cloud və s. göstərmək olar [5].

IaaS virtualaşdırma texnologiyasına əsaslanır və istifadəçiyə avadanlığı mövcud fəaliyyət ehtiyaclarına müvafiq olan hissələrə bölmək imkanı verir, bununla da mövcud hesablama imkanlarının istifadəsinin səmərəliliyini artırır. İstifadəçi server vaxtını, disk həcmi və digər resursları ona işləmək üçün zəruri olan miqdarda sərf edəcək. Bundan başqa, IaaS müştəriyə bütün nəzarət funksiyalarını vahid bir platformada təqdim edir [1]. İstifadəçinin işi strukturu idarə etmək deyil, əməliyyat sisteminə, yaradılmış proqrama nəzarət etməkdir [6].

- *Platform-as-a-service (PaaS) – platforma xidməti kimi.*

PaaS servisi istifadəçilərə virtual serverlərdə (fiziki serverlərdən təşkil olunan) yerləşən əməliyyat sistemlərindən və xüsusiləşdirilmiş proqram əlavələrindən (Apache, My SQL və s.) istifadə etməsinə imkan yaradan virtual platformadır. Paas servisinə misal olaraq IBM İT Factory, Google App Engine, Microsoft.NET Azure Services Platform (Windows Azure), Force.com xidmətlərini göstərə bilərik [5].

Veb-tətbiqlərin yaradılması, sınaqdan keçirilməsi, yerləşdirilməsi və dəstəklənməsi üçün vahid bir platforma kimi PaaS bütün əməliyyatları vahid inteqrasiya olunmuş mühitdə təmin edir, bununla da ayrı-ayrı mərhələlərdə müxtəlif mühitlərin dəstəklənməsinə sərf edilən xərcləri aradan qaldırır [1]. Bu xidmət növündə müştərinin cloud infrastrukturunu üzrə satın alınmış funksional proqramları yerləşdirmək hüququ vardır. Burada da müştəri şəbəkə, server kimi cloud strukturunu idarə etmir və yoxlamır. O sadəcə, burada quraşdırdığı funksional proqrama nəzarət edir [7, 8].

- *Software-as-a-service (SaaS) – proqram təminatı kimi*

Bu xidmət istifadəçiləri proqram təminatı ilə təmin edir. Bu səviyyədə istifadə olunan proqramlara misal olaraq Microsoft “Software Services” (e-mail, video konfrans), Google Apps, Google Docs və s. göstərmək olar. İstifadəçi ona lazım olan proqram əlavələrinin rezident hissəsini öz kompüterinə yükləmədən şəbəkə kanallarının köməyi ilə buludlara müraciət edir.

Proqram əlavələri SaaS xidməti verən təchizatçının serverində işləyir və istifadəçiyə hesablamaların nəticəsini göndərir. Beləliklə, istifadəçi proqram təminatını almır və lazım gələndə ondan məsələnin həllində istifadə edir və istifadəyə görə uyğun pul ödəyir [5].

SaaS konsepsiyasına əsasən, istifadəçi bir məhsulu satın alaraq eyni zamanda onun üçün ödəniş etmir, onu kirayə götürür. Bundan başqa, o, məhz ona lazım olan funksiyalardan istifadə edir. Məsələn, bir proqram sizə ildə bir dəfə lazım olur. Bu proqramdan bundan çox istifadə etmək niyyətində deyilsiniz. Beləliklə, lazımsız proqramın sizin kompüterinizdə yer tutmasına ehtiyac qalmır. SaaS məntiqi WaaS (WaaS - bir xidmət kimi iş yeri) anlayışına əsaslanmışdır. Yəni, müştəri proqram təminatı ilə işləmək üçün tam təmin olunmuş virtual iş yeri ilə təchiz olunur [9].

AzScienceNet şəbəkəsində cloud computing xidmətinin qurulması məsələləri

Hazırda dünyada superkompüterlərin yerinə yetirdiyi işləri həyata keçirən, eyni zamanda daha ucuz başa gələn cloud computing sistemlərinin yaradılması üzrə intensiv tədqiqat işləri aparılır. Böyük hesablamalar həyata keçirən belə sistemlər yüksək sürətli əlaqə kanalına malik olan kompüter şəbəkələri əsasında yaradılır. Yüksək sürətli əlaqə kanallarından istifadə etməklə, müxtəlif təşkilat və müəssisələrin istifadəçilərinin Cloud computing sisteminin xidmətlərindən istifadə etməsi iqtisadi cəhətdən daha sərfəlidir.

AzScienceNet şəbəkəsinin Data Mərkəzinin qurulması ən son texnologiyalar əsasında təşkil edilmişdir. Data Mərkəzin qurulmasında IBM şirkətinin avadanlıqlarından istifadə olunmuşdur.

- Bleyd serverlər –53 ədəd;
- Hesablama qovşaqlarının sayı – 808 Core;
- Əməli yaddaşın həcmi – 4.3 Tbayt;
- Xarici yaddaşın həcmi – 146.4 Tbayt;
- Hesablama məhsuldarlığı – 14.8 Tflops [3].

Bu avadanlığın köməyi ilə hər biri minimum 2 nüvəli prosessor olmaqla eyni zamanda 284 istifadəçini virtual resursla təmin etmək mümkündür.

AzScienceNet şəbəkəsi hal-hazırda 2500 istifadəçiyə çoxsaylı İnternet xidmətləri (İnternet, hosting, elektron poçt, elektron kitabxana, distant təhsil, AzScienceCERT, Eduroam, Cloud computing və s.) göstərir.

Cloud computing texnologiyası istifadəçilərə güclü hesablama və böyük yaddaş resursları əldə etməyə imkan verir və eyni zamanda bu resursların harada yerləşməsi və sazlanması istifadəçini maraqlandırmır.

Hal-hazırda AzScienceNet şəbəkəsi üzərində IaaS xidmətinin istifadəsinə başlanılmışdır. AzScienceNet-in cloud xidmətlərinə çıxış üçün istifadəçilərin ilkin olaraq www.azsciencenet.az səhifəsinə, buradan “AzCloud” keçidinə və ya İnternet brauzerdə birbaşa olaraq www.cloud.azsciencenet.az ünvanına daxil olması lazımdır.

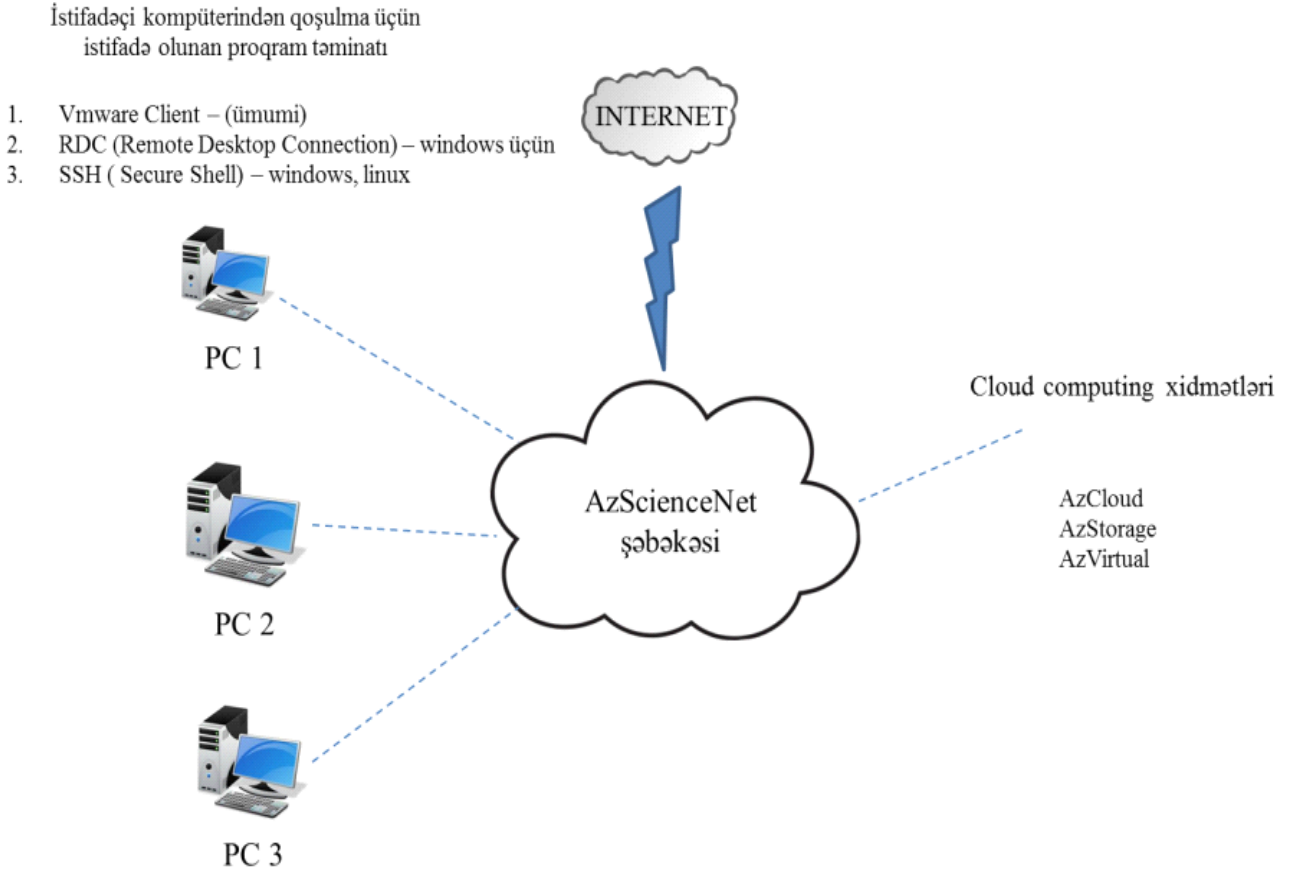
AzCloud-un platforması İBMSmartCloudur. IBM SmartCloud proqramı RedHat Linux Enterprise üzərində qurulur. Bu proqram IBM şirkətinin sırf cloud üzrə ixtisaslaşmış məhsuludur. Bu proqramın üzərində müxtəlif tipli və parametirli əməliyyat sistemləri qurmaq mümkündür. Hal-hazırda istifadəçilərə 5 müxtəlif konfigurasiya təklif olunur;

- Xsmall (ən kiçik) 2 Virtual CPU, 2048 MB Əməli yaddaş, 50 GB Yaddaş;
- Small (kiçik) 2 Virtual CPU 4096 MB Əməli yaddaş 50 GB Yaddaş;
- Medium (orta) 4 Virtual CPU, 4096 MB Əməli yaddaş, 50 GB Yaddaş;
- Large (böyük) 4 Virtual CPU, 6144 MB Əməli yaddaş, 50 GB Yaddaş;
- XLarge (ən böyük) 8 Virtual CPU, 8192 MB Əməli yaddaş, 50 GB Yaddaş

Təklif olunan əməliyyat sistemləri aşağıdakılardır: Windows 2008 R2, Windows 7 x64, CentOS, RedHat Enterprise 6.2.

Eyni zamanda, Data Mərkəzin virtual hesablama və yaddaş resurslarından istifadə etmək üçün Vmware proqram təminatından da istifadə olunur. Hazırda bu proqram təminatının köməyi ilə Data Mərkəzin istifadəsiz qalan resurslarının istifadəçilər arasında paylaşılması məsələsi həll olunur. Məsələnin həlli yolları aşağıdakı kimidir [3]:

İstifadəçi Data Mərkəzin resurslarından istifadə etmək üçün kompüterinə VMware Client (RDS – Remote Desktop Connection, SSH – Secure Shell və s.) proqramlarını yükləməlidir. Bundan sonra istifadəçi öz fərdi kompüterinin həll etməyə gücü çatmadığı mürəkkəb məsələlərin həlli üçün Data Mərkəzin resursları əsasında lazımı virtual maşınla təmin edilir (şəkil 1).



Şəkil 1. Data Mərkəzdə hesablama və yaddaş resurslarının virtuallaşdırılması sxemi

Data Mərkəzdə AMEA-nın institut və təşkilatları üçün fayl arxivinin yaradılması istiqamətində işlər görülmüşdür. Belə ki, Data Mərkəzdə hər bir qurum üçün xüsusi yaddaş resursu ayrılmışdır. Bu resurslar yalnız həmin istifadəçilərin daxil ola biləcəyi formada istifadəçi adına görə bölünmüşdür və şifrə ilə qorunur. Bununla da həm quruma aid olan şəxsi faylların itmə və məhv olma təhlükəsi ilə üzləşməsinin qarşısı alınır, həm də hər qurumun yaddaş resursları üçün ayrıca avadanlığın alınması kimi izafi xərclərdən azad olmuş oluruq [3].

AzScienceNet şəbəkəsində cloud və virtual resursların təhlükəsizlik məsələləri və onların həlli yolları

Şəbəkədə cloud və virtual resurslardan istifadə zamanı istifadəçilərin məlumatlarının etibarlılığını təmin etmək üçün bir neçə təhlükəsizlik üsulundan istifadə edilir.

1) *DDoS və buna bənzər hücumlar. Serverlərə göndərilən çoxsaylı sorğular.*

Xüsusi quraşdırılmış təhlükəsizlik monitoring sistemi Data Mərkəzin trafikini tam olaraq analiz edir və hücumların qarşısını alır. Bu hücumlar bir neçə hissəyə bölünür:

- Proqram təminatına edilən ənənəvi hücumlar. Bu tip təhlükələr şəbəkə protokollarında, əməliyyat sistemlərində boşluqlar olduğu zaman meydana gəlir. Bu təhdidlərdən qorunmaq üçün AzScienceNet şəbəkəsində antivirus, şəbəkəarası ekran, müdaxilələri aşkarlama sistemindən istifadə olunur.
- Cloudun elementlərinə edilən funksional hücumlar. Bu tip hücumlar cloudun çoxlaylı olması, təhlükəsizlik prinsiplərinin ümumi olması ilə əlaqədardır. Bunun qarşısının alınması üçün clouddan əvvəl əks proksi quraşdırılmışdır. DoS - hücumun uğur qazanması bütün clouda olan girişi bloklayır, lakin cloudun daxilində bütün əlaqələr və funksiyalar işlək vəziyyətdə qalır.
- Kliyəntə edilən hücumlar. Bu tip hücum veb mühit üçün səciyyəvidir, lakin cloud üçün də aktual hesab olunur. Çünki kliyənlər clouda brauzerlər vasitəsilə qoşulurlar. Bu sinif hücumlara Cross Side Scripting, veb-sessiyaların tutulması, parolların oğurlanması və s. aid edilir. Bu hücumlardan qorunmaq üçün ənənəvi olaraq ciddi autentifikasiya üsulundan və qarşılıqlı autentifikasiya zamanı şifrələnmiş əlaqədən istifadə edilir [10].

2) *Parolun yığım metodları ilə ələ keçirilməsi riski.* Xüsusi proqram vasitəsi ilə digər şəxsə aid olan parolun müxtəlif variantlarda yığılaraq tapılması.

- Hər hansı bir kənar şəxs tərəfindən parolun yığım metodları ilə ələ keçirilməsi riskinin qarşısının alınması üçün istifadəçilərə parol dəyişikliyini zamanı məhdudiyətlər qoyulur. Bu məhdudiyətlərə paroldakı simvolların sayı və müxtəlifliyi (böyük və kiçik hərflər, rəqəmlər və simvollar) aiddir. Lakin etibarlılığın yüksək səviyyəsini təmin etmək üçün sertifikat və tokenlərdən istifadə edilir. LDAP və SAML kimi standartlardan istifadə edilməsi məqsəduyğundur.
- İstifadəçi virtual resursa qoşulmaq üçün özünə məxsus olan IP ünvanından istifadə etməlidir.
- Hər bir virtual resursun hesabat tipli qrafikləri daim analiz olunur və qeyri-normal tendensiya müşahidə olunan zaman administrator xəbərdar olunur.

3) *Konfidensial məlumatların 3-cü şəxslər tərəfindən mənimsənilməsi təhlükəsi.*

Sistemdə qeydiyyat (log) aparan servislər vardır. Bu servislər sistemdə aparılan bütün dəyişiklikləri, giriş-çıxışları və görülən işləri qeydiyyata alır [11]. Bir sözlə, informasiyanın sürətinin çıxarılması, silinməsi və s. hallarında bu əməliyyatın nə zaman və kim tərəfindən edildiyini aydınlaşdırmaq mümkündür. Bundan əlavə istifadəçi virtual resurslardan istifadə edib öz işini tamamilə sonlandırdıqdan sonra onun məlumatları geri qaytarılması mümkün olmayacaq şəkildə silinir.

4) *Fiziki serverlərin oğurlanması və ya sınması halları.*

Məlumatlar cloudda saxlanılan kimi dərhal onların bir nüsxəsi avtomatik olaraq bir neçə serverə paylanır. Bu serverlər struktura görə eyni data mərkəzdə və ya müxtəlif data mərkəzlərdə yerləşə bilər. Belə ki, sınma və ya oğurlanma halları baş verdikdə istifadəçinin məlumatları itmir.

5) *Məlumatların itməsi təhlükəsi və qəza hallarından sonra bərpa.*

Qəza halları və məlumat itkisi. Data mərkəzdə belə halların qarşısının alınması üçün bütün virtual əməliyyat sistemlərinin və məlumatların ehtiyat nüsxələri çıxarılır. Bir qəza olduğu zaman qısa zamanda itmiş və ya məhv olmuş məlumatlar geri qaytarılır. Bu məsələnin bir neçə üsulla həlli mövcuddur:

- Ümumi backup sistemi vasitəsilə bütün məlumatların ehtiyat nüsxələrinin çıxarılması. Xüsusi proqramlar vasitəsilə virtual maşınların və storage-da yerləşən istifadəçi fayllarının ehtiyat nüsxələri çıxarılaq yaddaş kasetlərinə (tape drive) yazılır.
- Virtual maşınların yerləşdiyi fiziki serverlərin proqram təminatlarında nasazlıq baş verdiyi zaman həmin serverin üzərində yerləşən virtual maşınlar avtomatik olaraq digər serverin üzərinə keçirilir. Bu proses zamanı heç bir fasilə baş vermir.
- Məlumatları virtual resursdan şəxsin öz kompüterinə köçürməsi. Yəni hər iş gününün sonunda virtual maşında həll olunan məsələnin nəticələri və ya orada olan lazımlı fayllar

istifadəçinin şəxsi kompüterinə yazılır. Data Mərkəzin təhlükəsizlik standartlarına görə onun yerləşdiyi məkandan kənarında ehtiyat Data Mərkəz (Disaster Recovery and Backup Center) olmalıdır ki, hər hansı bir fəvqəladə hal zamanı fəaliyyət oradan davam etsin və məlumat itkisi olmasın. Hal-hazırda AzScienceNet-də vahid Data Mərkəzi olduğundan təhlükəsizlik üçün bu metoddan istifadə olunur.

6) Rabitə kanalı ilə ötürülən məlumatların digər şəxslər tərəfindən tutulması.

Ötürülən verilənlərin ilk növbədə şifrələnməsi təmin olunur. Bu məlumatları istifadəçi yalnız autentifikasiya prosesini keçdikdən sonra əldə edir. Bu prosedurların həyata keçirilməsi zəmanət verir ki, şəbəkənin etibarsız qovşaqlarından giriş əldə edən istənilən şəxs onların üzərində hər hansı dəyişiklik edə bilməsin. Bu əməliyyatlar TLS, IPsec və AES kimi etibarlı protokollar və alqoritmlər vasitəsilə həyata keçirilir [11, 12].

Nəticə

Məqalədə kompüter şəbəkələri əsasında paylanmış hesablama sistemlərinin yaradılması üçün istifadə edilən cloud computing texnologiyaları analiz olunmuş və servis xidmətlərinin təhlili aparılmışdır. Bu xidmətin AzScienceNet şəbəkəsində yaradılması şəbəkəyə qoşulan istifadəçilərin böyük hesablama və yaddaş resursları ilə təmin olunmasına imkan verir. Eyni zamanda, cloud və virtual hesablama və yaddaş resurslarından istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.

Ədəbiyyat

1. Введение в облачные вычисления.
http://www.intuit.ru/studies/courses/673/529/lecture/11913_.
2. Джонс Т. Cloud computing и Linux (Платформы и приложения для Cloud Computing).
www.ibm.com/developerworks/ru/library/ .
3. Ələkbərov R.Q., Həşimov M.A. AzScienceNet şəbəkəsində cloud computing texnologiyalarının tətbiqi perspektivləri haqqında // İnformasiya texnologiyaları problemləri, 2012, №2, s.30–36.
4. Takabi H., Joshi J.B.D., Ahn G. Security and Privacy Challenges in Cloud computing Environments // IEEE Security Privacy Magazine, 2010, vol 8, pp.24–31.
5. Semyonov Y.A. Telecommunication technologies. 2010, www.book.itep.ru
6. Sachdeva K. Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.
7. Winkler J.R. Securing the Cloud: Cloud Computer Security Techniques and Tactics. Elsevier Publishing, 2011.
8. Pearson S. Privacy, Security and Trust in Cloud computing, HP Laboratories, 2012.
9. Soleimanian F., Hashemi S. Security Challenges in Cloud computing with More Emphasis on Trust and Privacy // International Journal of Scientific & Technology Research, 2012, vol. 1, no. 6, pp.49–54.
10. Top threats to cloud computing V 1.0. Cloud Security Alliance, 2010.
11. Əliquliyev R.M., Abdullayeva F.C. Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya texnologiyaları problemləri, 2013, №1, s.3–14.
12. Security guidance for critical areas of focus in cloud computing. CloudSecurityAlliance, 2011.

УДК 004.75

Алекперов Рашид Г.¹, Гашимов Мамед А.², Мустафаев Турал И.³

Институт Информационных Технологий НАНА, Баку, Азербайджан

¹rashid@iit.ab.az; ²mhashimov@iit.ab.az; ³tural.mustafayev@iit.ab.az

Вопросы безопасности услуг Cloud computing и пути их решения

В статье анализируются принципы развития распределенных вычислительных систем, основанные на технологии облачных вычислений, и проблемы безопасности, возникшие в результате использования облака и виртуальных ресурсов в AzScienceNet, и пути их решения.

Ключевые слова: облачные вычисления, память и вычислительные ресурсы, вычислительные услуги, безопасность услуг облачных вычислений.

Rashid Q. Alakbarov¹, Mammad A. Hashimov², Tural I. Mustafayev³

Institute of Information Technology of ANAS, Baku, Azerbaijan

¹rashid@iit.ab.az, ²mhashimov@iit.ab.az, ³tural.mustafayev@iit.ab.az

Cloud computing service security issues and their solutions

The paper analyzes the development principles of distributed computing systems based on cloud computing technology, and security problems emerged from the use of cloud and virtual resources in AzScienceNet, and their solutions.

Keywords: cloud computing, memory and computing resources, computing services, cloud computing service security.