AzScienceNet şəbəkəsində Cloud computing xidmətinin təhlükəsizlik məsələləri və həlli yolları

Rəşid Ələkbərov[1], Məmməd Həşimov[2], Tural Mustafayev[3]

AMEA İnformasiya Texnologiyaları İnstitutu

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

***Xülasə*— Məqalədə hesablama buludları texnologiyaları əsasında paylanmış hesablama sistemlərinin yaradılması prinsipləri, AzScienceNet şəbəkəsində cloud və virtual resurslardan istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.**

Açar sözlər—hesablama buludu; yaddaş və hesablama resursları; hesablama servisləri; hesablama buludları xidmətlərinin təhlükəsizliyi

I. GİRİŞ

Kompüter şəbəkələri əsasında mürəkkəb məsələlərin həlli üçün paylanmış hesablama sistemlərinin yaradılmasında cloud computing texnologiyalarından geniş istifadə olunur. Böyük hesablama və yaddaş resurslarına malik olan bu cür sistemlər yüksəksürətli əlaqə kanalına malik olan kompüter şəbəkələri əsasında yaradılır. Yüksəksürətli əlaqə kanallarından istifadə etməklə, müxtəlif təşkilat və müəssisələrin istifadəçilərinin Cloud Computing sisteminin xidmətlərindən yararlanması iqtisadi cəhətdən daha sərfəlidir. Beləliklə, Cloud Computing – kommunikasiya texnologiyalarının köməyi ilə böyük təşkilatlarda yerləşən çoxsaylı kompüterlərin (server, kompüter, data mərkəz və s.) hesablama və yaddaş resurslarının klasterləşməsi və virtuallaşdırılmasını həyata keçirməklə, istifadəçilərin verilənlərinin emalı və yadda saxlanmasına xidmət edən hesablama sistemidir [1].

II. AZSCIENCENET ŞƏBƏKƏSİNDƏ CLOUD COMPUTING XİDMƏTİNİN TƏTBİQİ MƏSƏLƏLƏRİ

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

- Bleyd serverlər –38 ədəd;
- Hesablama qovşaqlarının sayı – 568 Core;
- Əməli yaddaşın həcmi – 2.8 T bayt;
- Xarici yaddaşın həcmi – 86.4 Tbayt;
- Hesablama məhsuldarlığı – 11 Tflops.

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 çoxsaylıİnternet xidmətləri (internet, hostinq, elektron poçt,elektron kitabxana, distant təhsil, AZ-CERT, Eduroam, Cloud computing və s.) göstərir.

Cloud Computing texnologiyası istfadəçilərə güclü hesablama və böyük yaddaş resursları əldə etməyə imkan verir və eyni zamanda bu resursların harda yerləşməsi və sazlanması istifadəçinin marağında olmur.

Cloud Computing istifadəçilərə10-dan artıq xidmət təklif edir. Ən çox istifadə olunan xidmətlər aşağıdakılardır [2]:

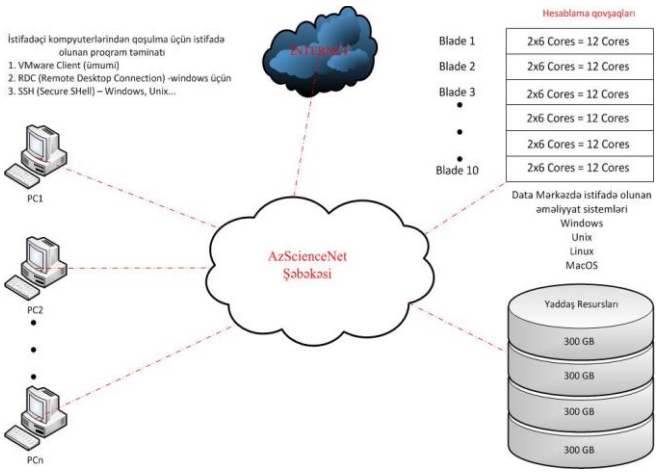
- İnfrastructure-as-a-service (İaaS) – infrastruktur xidmət kimi;
- Platform-as-a-service (PaaS) – platforma xidmət kimi;
- Software-as-a-service (SaaS) – proqram təminatı xidmət kimi.

Hal-hazırda AzScienceNet şəbəkəsi üzərində birinci xidmətin (İnfrastructure-as-a-service – hesablama və yaddaş resursları xidməti) istifadəsinə başlanılmışdır. İstifadəçilər AzScienceNet.az saytına daxil olmaqla AzCloud bölməsində qeydiyyatdan keçməklə müəyyən hesablama resursları əldə edə bilərlər (Şəkil 1).

Şəkil 1. AzScienceNet.az saytının AzCloud bölməsi

Eyni zamanda Data Mərkəzin virtual hesablama və yaddaş resurslarından istifadə etmək üçün Vmware proqram təminatındanda istifadə olunur. Bu proqramın əsas məqsədi administrator tərəfindən serverlərin resurslarının düzgün idarə olunmasında geniş istifadə etməkdir. Hazırda bu proqram təminatının köməyi ilə Data Mərkəzin istifadəsiz qalan resurslarının istifadəçilər arasında paylanması məsələsi həll olunur. Məsələnin həlli yolları aşağıdakı kimidir.

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 lazımi virtual maşınla təmin edilir (şəkil 2).



Şəkil 2. Data Mərkəzdə hesablama və yaddaş resurslarının virtuallaşdırılması sxemi

Data Mərkəzdə AMEA-nın institut və təşkilatları üçünfayl 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. Bununlada həm quruma aid olan şəxsi faylların itmə və məhv olma təhlükəsiylə üzləşməsinin qarşısı alınır, həm də hər qurumun yaddaş resursları üçün ayrıca avadanlığın alınması kimi izafi xərclərdən azad olmuş oluruq.

Cloud və virtual resurslarının istifadəsi zamanı təhlükəsizlik məsələləri ön plana çəkilir.

III. AZSCIENCENET ŞƏBƏKƏSİNDƏ CLOUD VƏ VİRTUAL RESURSLARIN TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ VƏ ONLARIN HƏLLİ YOLLARI

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

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

a) Proqram təminatına edilən ənənəvi hücumlar. Bu tip təhlükələr şəbəkə protokollarında, əməliyyat sistemlərində boşluqlar olduğu zaman meydana gəlir. Bu təhdidlərdən qorunmaq üçün bizim şəbəkəmizdə antivirus, şəbəkəarası ekran, müdaxilələri aşkarlama sistemindən istifadə olunur.

2) 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 buna baxmayaraq cloudun daxilində bütün əlaqələr və funksiyalar işlək vəziyyətdə qalır.

3) Kliyentə edilən hücumlar. Bu tip hücum veb mühit üçün səciyyəvidir, lakin cloud üçün də aktual hesab olunur. Çünki kliyentlər 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 [3].

2) Parolun yığım metodlarıyla ələ keçirilməsi riski.

Xüsusi proqram vasitəsiylə digər şəxsə aid olan parolun müxtəlif variantlarda yığılaraq tapılması.

a) Hər hansı bir kənar şəxs tərəfindən parolun yığım metodlarıyla ələ keçirilməsi riskinin qarşısının alınması üçün istifadəçilərə parol dəyişikliyi zamanı məhdudiyyətlər qoyulur. Bu məhdudiyyətlərə görə parolda istifadə olunan simvolların sayına və müxtəlifliyinə müəyyən tələblər qoyulur. Lakin etibarlılığın yüksək səviyyəsini təmin etmək üçün sertifikat və tokenlərdən istifadə edilir. LDAP və SAML kimi standartlardan istifadə edilməsi məqsədə uyğundur.

b) İstifadəçi virtual resursa qoşulmaq üçün özünə məxsus İP ünvandan istifadə etməlidir.

c) Hər bir virtual resursun hesabat tipli qrafikləri daimi analiz olunur və qeyri-normal tendensiya müşahidə olunan zaman administrator xəbərdar olunur.

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

Sistemdə qeydiyyat (loq) aparan servislər vardır. Bu servislər sistemdə aparılan bütün dəyişiklikləri, giriş-çıxışları və görülən işləri qeydiyyata alır. Bir sözlə informasiyanın surətinin çıxarılması, silinməsi və s. hallarında bu əməliyyatın nə zaman və kim tərəfindən olunduğunu aydınlaşdırmaq mümkündür. Bundan əlavə istifadəçi virtual resurslardan istifadə edib öz işini tamamladıqdan 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 vəya müxtəlif data mərkəzlərdə yerləşə bilər. Belə ki, sınma vəya 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 vəya məhv olmuş məlumatlar geri qaytarılır. Bu məsələnin bir neçə üsulla həlli mövcuddur:

a) Ümumi backup sistemi vasitəsilə bütün məlumatların ehtiyat nüsxələrinin çıxarılması. Xüsusi proqramlar vasitəsilə virtual maşınların və storage-da yerləşən istifadəçi fayllarının ehtiyat nüsxələri çıxarılaraq yaddaş kasetlərinə (tape drive) yazılır.

b) 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 qeydə alınmır.

c) Məlumatları virtual resursdan şəxsin öz kompüterinə köçürməsi. Yəni hər iş gününün sonunda virtual maşında həll olunan məsələnin nəticələri vəya orada olan lazımlı fayllar istifadəçinin şəxsi kompüterinə yazılır. Data Mərkəzin təhlükəsizlik standartlarına görə onun yerləşdiyi məkandan kənarda ehtiyat Data Mərkəz (Disaster Recovery and Backup Center) olmalıdır ki, hər hansı bir fövqəladə hal zamanı fəaliyyət oradan davam etsin və məlumat itkisi olmasın. Hal-hazırda bizim vahid Data Mərkəzimiz olduğundan təhlükəsizlik üçün bu metoddan istifadə olunur.

6) Rabitə kanalı ilə ötürülən məlumatların digər şəxs 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 [4].

NƏTİCƏ

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 istifadəçilərə böyük hesablama və yaddaş resursları ilə təmin olunma imkanları verir. Eyni zamanda cloud, virtual hesablama və yaddaş resurslarından istifadə zamanı meydana çıxan təhlükəsizlik problemləri və onların həlli yolları analiz olunmuşdur.

ƏDƏBİYYAT

[1] Джонс Т. Cloud Computing и Linux (Платформы и приложения для Cloud Computing). www.ibm.com/developezworks/ru/library/

[2] Ю.А.Семенов. Telecommunication technologies. 2010.www.book.itep.ru

[3] Top threats to cloud computing V 1.0. cloud security alliance, 2010

[4] Security guidance for critical areas of focus in cloud compiting. Cloud security alliance, 2011