Qrid sistemlərində təhlükəsizlik texnologiyalarının analizi

Rəşid Ələkbərov[1], Səməd Dursunov[2]

[1,2] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

[1]t.direktor_muavini@iit.science.az, [2]samed.dursunov@iit.science.az

***Xülasə*– Məqalədə böyük hesablama resursları tələb edən mürəkkəb məsələlərin həllində istifadə olunan paylanmış hesablama sistemlərinin təhlükəsizlik sistemləri təhlil olunmuşdur. Qrid sistemlərində istifadə edilən təhlükəsizlik standartları, paylanmış hesablama mühitində təhlükəsizlik sistemlərinə olan tələblər və Qrid sistemlərinin təhlükəsizlik arxitekturası haqqında geniş məlumat verilmişdir.**

Açar sözlər – paylanmış hesablama, Qrid, təhlükəsizlik sistemləri, təhlükəsizlik protokolları, X.509.

I. GİRİŞ

Müasir dövrdə İnternetə qoşulmuş kompüterlər əsasında yaradılan yüksək məhsuldarlıqlı paylanmış hesablama sisteminə daha perspektivli sistemlər kimi baxılır. Etibarlılığın yüksəlməsi, əlaqə kanallarında məlumatın ötürmə sürətinin artması, informasiya texnologiyaları və şəbəkə avadanlıqlarının sürətli inkişafı şəbəkələrdə cəmlənmiş kompüterlərin hesablama gücünün artmasına gətirib çıxarmışdır. Qeyd etmək lazımdır ki, elmin müxtəlif sahələrində meydana çıxan böyük hesablama və yaddaş resursları tələb edən mürəkkəb məsələlərin həllində fərdi kompüterlərin hesablama gücü kifayət etmir. Göstərilən məsələlərin həllində yüksək hesablama məhsuldarlığına və böyük yaddaşa malik olan superkompüterlərdən geniş istifadə edilir. Strateji məhsul sayılan superkompüterlərin qiymətlərinin baha olması bir cox ölkələrin onları əldə etməsinə və elmi-texniki tədqiqat işlərində istifadə etməsinə imkan vermir. Bununla yanaşı şəbəkəyə qoşulmuş yüz milyonlarla kompüterlərin hesablama və yaddaş resurslarından səmərəli istifadə olunmur. Aparılan tədqiqatlar göstərir ki, hər bir istifadəçi fərdi kompüterin imkanlarının yalnız 25-30%-in istifadə edir. Belə olan təqdirdə, fərdi kompüterlərin istifadəsiz qalan hesablama və yaddaş resurslarından mürəkkəb məsələlərin həllində istifadə etmək daha məqsədə uyğun olardı.

Qrid mühiti müxtəlif aparat-proqram platformalardan ibarətdir. O personal kompüterlər, işçi stansiyaları, meynfreymlər və super EHM-lər əsasında qeterogen mühit yaradır. Belə bir mühitdə əsas həll olunmalı problemlərdən biri də resursların idarə olunmasıdır, informasiya təhlükəsizliyinin təmin olunması və mühitin şəffaflığının təmin olunmasıdır. Şəffaflıq deyiləndə məlumat mübadiləsi, tətbiqi proqramların internet üzərindən əlyetərliyi, sistemlərin uzaqdan idarə olunması və s. kimi əməliyyatların razılaşdırılmış protokollar əsasında aparılması başa düşülməlidir. Bu keyfiyyətlərə nail olmaq üçün, Qrid mühiti açıq sistemlər prinsipi ilə qurulmalıdır. Sistemin açıq olmasını təmin etmək üçün bir sıra addımlar atmaq, üsul və vasitələrdən istifadə etmək lazımdır. Yəni açıq sistem texnologiyası adlanan müəyyən bir texnologiyanı istifadə etmək lazımdır.

Yuxarıda qeyd olunanlar və bu sahədə aparılmış araşdırmalar əsasında demək olar ki, dünyada mürəkkəb məsələlərin həllində digər sistemlərlə yanaşı daha az vəsait hesabına başa gələn paylanmış hesablama sistemlərindən geniş istifadə olunur.

Təqdim olunmuş işdə həmin sistemlərin təhlükəsizliyinin təmin olunması məsələləri araşdırılmışdır [1].

II. QRİD SİSTEMLƏRİNDƏ İSTİFADƏ EDİLƏN TƏHLÜKƏSİZLİK STANDARTLARI

Bu bölmədə mövcud standartlar və onların Qrid sistemlərinin tələblərinə cavab vermə dərəcəsinə baxılmışdır [2,3].

1. Kerberos – IETF standartıdır. Bu standart sistemin təhlükəsizliyini doğruluq, tamlıq və ötürülən informasiyanın məxfiliyi əsasında dəstəkləyir. Bu protokol birdəfəlik avtorizasiyanı və ötürülən informasiyanın çevik qorunmasını təmin edə bilər. Lakin bu protokolun tətbiqi üçün vacib olan inteqrasiya tələbləri ilə lokal təhlükəsizlik həllərini uzlaşdırmaq çətindir. Ona görə ki, Kerberos tətbiqinin daxili təhlükəsizlik həllərini dəyişmək xüsusiyyəti vardır.
2. TLS (Transport Layer Security) – IETF standartıdır və doğruluq, tamlıq və ötürülən informasiyanın məxfiliyini təmin edir. Bu standart açıq açar kriptoqrafiyası texnologiyası ilə yaradılıb. Bu protokolun istifadəsi birdəfəlik avtorizasiya və ötürmə tətbiq etdikdə mümkün deyil.
3. PKIX (Public key infrastructure) – açıq açar infrastrukturu və imtiyazların idarə olunması infrastrukturu üçün olan ITU-T standartıdır. X.509 standartları adətən digər təhlükəsizlik standartları (məsələn TLS) ilə birlikdə istifadə olunur.
4. CMS (Cryptografic Message syntax) – IETF standartıdır. Bu standart rəqəmsal imza, autentifikasiya və ya hər hansı rəqəmsal məlumatların şifrələnməsi üçün istifadə olunur.
5. GSS-API (Generic Security Service API) – oxşar təhlükəsizlik xidmətlərinin uyğunsuzluq problemlərini aradan qaldırmaq üçün nəzərdə tutulub. Bu standart əsas

DOI: 10.25045/NCInfoSec.2017.20

təhlükəsizlik mexanizmlərindən biri ilə paylanmış hesablama mühitində istifadə edilə bilər [2,3].

III. PAYLANMIŞ HESABLAMA MÜHİTİNİN TƏHLÜKƏSİZLİK SİSTEMLƏRİNƏ OLAN TƏLƏBLƏR

Paylanmış hesablama sistemlərinin inkişafında dünya təcrübəsinin təhlili göstərir ki, Qrid təhlükəsizlik sistemi aşağıdakı xüsusiyyətlərə malik olmalıdır:

1. İstifadəçilərin birdəfəlik qeydiyyatını aparma imkanı - belə qeydiyyatı, istifadəçi ancaq sistemə daxil olduqda identifikasiya prosedurunun yerinə yetirilməsini nəzərdə tutur. Paylanmış hesablama mühitinin resursları arasında bu istifadəçinin bütün keçidləri təkrar identifikasiya olunmadan həyata keçirilir [4,5].

2. Hüquqların ötürülməsi imkanı - hüquqların ötürülməsi o deməkdir ki, istifadəçinin avtorizasiya olunduğu resurslardan istifadə etməyə, habelə hüquqlarını alt proseslərə ötürməyə icazəsi olmalıdır.

3. Lokal təhlükəsizlik sistemləri ilə inteqrasiya imkanı - hər bir resurs sistemin təhlükəsizlik problemini mövcüd olan təhlükəsizlik həllərindən birini istifadə etməklə həll edə bilər. Qrid təhlükəsizlik sistemi lokal sistemlərin təhlükəsizliyini dəyişdirmədən onlarla qarşılıqlı əlaqə qurmalıdır.

4. Etibarlılıq əlaqələri həyata keçirmək bacarığı - etibarlılıq münasibətinə görə, əqər istifadəçi A resursunda avtorizasiyadan keçibsə və A resursu B resursu ilə qarşılıqlı əlaqədədirsə, onda həmin istifadəçi B resursunda avtorizasiya olunmuş hesab olunmalıdır.

IV. QRİD SİSTEMLƏRİNİN TƏHLÜKƏSİZLİK ARXİTEKTURU

Qrid sistemləri özündə daima böyüyən güclü hesablama resursları və iri tutumlu saxlama resurslarını birləşdirir. Həmin resurslara girişlərin idarə olunması təhlükəsizlik nöqteyi nəzərindən Qrid sistemlər üçün əsas problemlərdən biridir.

Təhlükəsizlik protokolları Qriddə istifadəçilərin birdəfəlik qeydiyyatı, proqramlara və xidmətlərə istifadəçi səlahiyyətlərinin ötürülməsi və s. kimi tələbləri yerinə yetirir.

Hal-hazırda Qrid təhlükəsizliyi infrastrukturu (Grid Security Infrastructure - GSI) mövcuddur [6]. Bu infrastruktur, qorunmayan ümumi girişi olan şəbəkələrin (İnternet), təhlükəsiz işləməsini təmin edir, autentifikasiya, məlumatların konfidensial ötürülməsi və Qrid sistemlərinə tək bir giriş xidmətlərini göstərir.

GSI etibarlı və geniş istifadə olunan açıq açar kriptoqrafiya infrastrukturuna əsaslanır (Public Key Infrastructure – PKI) [5,7].

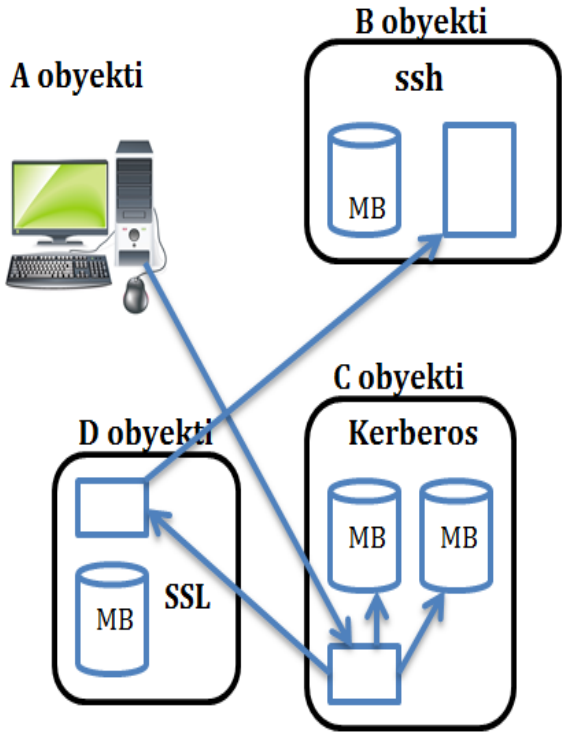
GSI-da identifikasiya - istifadəçilərin və resursların identifikatoru kimi X.509 rəqəmsal sertifikatlar istifadə olunur. X.509 sertifikatları ilə işləyərkən və sertifikatların verilməsi / qəbul edilməsi qaydasında üç tərəf iştirak edir:

1. Sertifikatlaşdırma mərkəzi (Certificate Authority – CA) - rəqəmsal sertifikatların verilməsi (imzalamaq) səlahiyyətinə malik xüsusi bir təşkilatdır.
2. Abunəçi – CA sertifikasiya xidmətlərindən istifadə edən bir şəxs və ya resursdur.
3. İstifadəçi – abunəçidən aldığı sertifikatın məlumatlarına arxalanan bir şəxs və ya resursdur.

Avtorizasiyanın idarə olunması Generic Authorization and Access interfeysi vasitəsi ilə həyata keçirilir və müxtəlif daxili təhlükəsizlik siyasətlərinin Qrid infrastrukturuna inteqrasiya olunmasına imkan verir (şifrələr, Kerberos sistemi və s. əsasında).

Səlahiyyətlərin həvalə edilməsi - məhdud müddətə hüquqların bir hissəsinin (sertifikatla müəyyən edilmiş qaydada), digər hesablama sistemində iştirakçının (müştəri) adından əməliyyatların aparılması üçün verilməsidir. Hüquqlar sertifikata sahib olduqda təsdiq olunur (müvafiq bağlı açarla). Ötürmə bağlı açarın ötürülməsi demək deyil (sertifikatla bir yerdə). Ötürmə o deməkdir ki, müştəri yeni proksi sertifikat imzalayır və bu sertifikat müştəri adından əməliyyatların aparılması üçün istifadə olunur. Müştərinin komponentində göstərmək yetərlidir ki, hansı növ Ötürmə (tam və ya məhdud) istifadə olunsun. Grid xidməti Ötürmə sertifikatı ala bilər və onun üzərindən sərəncam verə bilər.

Şəkil 1-də Qrid sistemlərində böyük miqyaslı paylanmış hesablama nümunəsi göstərilmişdir. Şəkildən göründüyü kimi istifadəçi müxtəlif obyektlərdə yerləşdirilmiş verilənlər və hesablama resurslarından istifadə etməklə qoyulmuş məsələni həll edir.



Şəkil 1. Böyük miqyaslı paylanmış hesablama nümunəsi.

NƏTİCƏ

Məqalədə paylanmış hesablama sistemlərində istifadə olunan təhlükəsizlik sistemləri haqqında geniş məlumat

verilmişdir. Qrid təhlükəsizlik texnologiyası, arxitekturası və protokolları ətraflı araşdırılmışdır. Qrid texnologiyasında istifadə olunan Qrid Təhlükəsizlik İnfrastrukturunun (Grid Security Infrastructure - GSI) hissələri və arxitekturasının təhlili aparılmışdır. GSI-da istifadə olunan PKI standartı olan X.509 rəqəmsal sertifikatın işləmə prinsipi göstərilmişdir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Qrant № EİF-2014-9(24)-KETPL-14/02/1**

ƏDƏBİYYAT

1. R.Q. Ələkbərov, M.A. Həşimov, ”Şəbəkə mühitində paylanmış hesablama sisteminin yaradılması texnologiyaları,” Ekspress-İnformasiya, Bakı, 2015, 74 s.
2. Каменщиков М.А. “Сервисы GRID, как объекты стандартизации” "ЖУРНАЛ РАДИОЭЛЕКТРОНИКИ" N 12, 2002 http://jre.cplire.ru
3. http://toolkit.globus.org/toolkit/
4. I.Foster C.Kesselman G.Tsudik S.Tuecke “A Security Architecture for Computational Grids”, CCS 98 Proceedings of the 5th ACM conference on Computer and communications security, San Francisco, California pp 83-92.
5. В.А. Галатенко “Анализ архитектурных аспектов информационной безопасности ГРИД-систем”, Международный научно-практический журнал Программные продукты и системы № 3 2010-ci il.
6. Maath.Kamal.Al-anni Gaining Secure Assets using Integrated Components of Grid Security Infrastructure (GSI) Creating inside Grid Environment, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 pp 291-296.
7. R. Butler, V. Welch, D. Engert, I. Foster, S. Tuecke, J. Volmer, C. Kesselman “A national-scale authentication infrastructure”, Journal IEEE Computer Society, Issue: 12, December 2000, pp 60-66.

ANALYSIS OF SECURITY INFRASTRUCTURE SYSTEM USED IN GRID TECHNOLOGIES

Rashid Alakbarov[1], Samed Dursunov[2]
[1,2] Institute of Information Technology,
Baku, Azerbaijan
[1]t.direktor_muavini@iit.science.az, [2]samed.dursunov@iit.science.az

Abstract – The article analyzes the security aspects of distributed computing systems used to solve complex issues requiring great computational resources. This paper provides extensive information on security standards used in Grid systems, requirements for security systems in distributed computing environments and security architecture of Grid systems.
Keywords – distributed computation, Grid, security systems, security protocols, X.509.