

E-elm mühitində informasiya təhlükəsizliyi problemləri

Təhmasib Fətəliyev¹, Yadigar İmamverdiyev²

AMEA İnformasiya Texnologiyaları İnstitutu

¹tfat@itsc.ab.az, ²yadigar@lan.ab.az

Xülasə— E-elm infrastrukturunu paylanmış, heterogen, hər birinin avtonom informasiya təhlükəsizliyi siyasəti olan müxtəlif inzibati domenlərdən ibarətdir. Bu domenlər arasında istifadəçilərin vahid identifikasiya sisteminin yaradılması vacib məsələdir. Bu işdə e-elm mühitində istifadəçilərin identifikasiyası modelləri analiz edilir, onların üstün və çatışmayan cəhətləri müəyyən edilir.

Açar sözlər— e-elm; informasiya təhlükəsizliyi; istifadəçilərin identifikasiyası; identifikasiya provayderi; servis provayderi

I. GİRİŞ

Müasir elmi tədqiqatlar hesablama sistemləri, elmi-tədqiqat alətləri, verilənlər bazaları, sensorlar, şəbəkələr və insanlar kimi coğrafi paylanmış və heterogen resursları birləşdirir. Belə böyük miqyaslı və geniş elmi tədqiqatlar qlobal miqyaslı əməkdaşlıq vasitəsilə həyata keçirilir ki, burada da informasiya və kommunikasiya texnologiyaları aparıcı rol oynayır; bu fenomen e-elm olaraq adlandırılır.

Azərbaycan Respublikasında 2009–2015-ci illərdə elmin inkişafı üzrə Milli Strategiya respublikada elmi infrastrukturun modernləşdirilməsi, tədqiqatların müasir standartlar səviyyəsində aparılması, elmin informasiya təminatının formalaşdırılması, beynəlxalq elmi əməkdaşlıq, elm və təhsilin inteqrasiyası və s. məsələləri aktuallaşdırmışdır. “Elektron elm” müasir İKT-nin imkanlarından geniş istifadə etməklə məhz bu məsələlərin həllini həyata keçirir [1].

E-elm infrastrukturunu üçün əsas tələblərdən biri informasiya təhlükəsizliyi və fərdi məlumatların mühafizəsi ilə bağlıdır. Azərbaycan Respublikası Prezidentinin “İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında” 26 sentyabr 2012-ci il tarixli fərmanı e-dövlətin mühüm bir infrastrukturunu kimi e-elm mühitində informasiya təhlükəsizliyinin etibarlı şəkildə təmin edilməsi məsələsini qarşıya qoyur [2].

E-elm mühiti üçün də informasiya təhlükəsizliyinin autentifikasiya, avtorizasiya, verilənlərin konfidensiallığının və tamlığının təmin edilməsi, protokollaşdırma və audit, ekranlama kimi baza texnologiyaları istifadə edilir, lakin onların e-elm mühitində həyata keçirilməsi bir sıra xüsusiyyətlərə malikdir.

Paylanmış, heterogen, əksər hallarda müxtəlif ölkələrin ərazisinə səpələnmiş bu infrastrukturda ən vacib məsələlərdən biri də istifadəçilərin etibarlı identifikasiyasını təmin etməkdir. Təqdim olunan işdə e-elm mühitində istifadəçilərin identifikasiyası modelləri analiz edilir, onların üstün və çatışmayan cəhətləri müəyyən edilir.

II. ELEKTRON ELM KONSEPSİYASI

Müasir elmi-tədqiqatlarda tədqiqat problemləri daha mürəkkəbdir, elmi-tədqiqat obyektini izolə etmək çətindir, o, elmin bir neçə sahəsini əhatə edir və geniş miqyaslıdır. Həmçinin elmi-tədqiqatlarda böyük həcmdə verilənlərdən intensiv istifadə edilir. Verilənlərin intellektual analizi, kompüter modelləşdirməsi lazımı, zəruri metodlara çevrilir, elmi tədqiqatçılar arasında daha çox kommunikasiya, əməkdaşlıq, koordinasiya ehtiyacı yaranır [3]. Bu məqsədlərlə İKT-nin elmdə geniş istifadəsi sayəsində elmi-tədqiqatların xarakterində, təşkilində, miqyasında, mürəkkəbliyində, həyat tsiklində, alətlərində bir sıra mühüm dəyişikliklər baş verir, elmi-tədqiqatların aparılmasının yeni texnologiyaları və alətləri yaradılır, yeni elmi-tədqiqat modeli və təşkilat modeli (virtual laboratoriya) meydana çıxır. Hazırda bu keyfiyyət dəyişikliklərini “e-elm” termini ilə xarakterizə edirlər (ABŞ-da “kiberinfrastruktur” termininə üstünlük verirlər) [4,5].

E-elm termini 1999-cu ildə Böyük Britaniya Elmi Şuralarının baş direktoru Con Teylor tərəfindən daxil edilib [6]: “E-elm – elmin aparıcı sahələrində qlobal əməkdaşlıq və buna imkan yaradan yeni nəsillər infrastruktur deməkdir.” Bu tərif əsasən texniki aspektlərə işarə edir: E-elm müxtəlif elm sahələrində, laboratoriyalarda, təşkilatlarda və ölkələrdə tədqiqatçıların qlobal əməkdaşlığını təmin edir, coğrafi paylanmış qeyri-bircins resursları – hadisələrin və proseslərin kompüter modellərini, hesablama sistemlərini, tədqiqat avadanlığını, elektron kitabxanaları, verilənlər bazalarını və informasiya resurslarının digər mənbələrini, sensorları, proqram vasitələrini, şəbəkə resurslarını əhatə edir. Son vaxtlar e-elm anlayışı daha çox İKT-nin elmə tətbiqinin sosial aspektlərini və nəticələrini xarakterizə etmək üçün işlədilir [7].

E-elmin uğurunun əsas səbəbi – mürəkkəb paylanmış sistemlərin yaradılmasına imkan verən, yüksək sürətli hesablama, nəhəng həcmdə verilənlərə sürətli girişi və səmərəli kommunikasiyaları dəstəkləyən yeni texnologiyaların sürətli inkişafıdır.

E-elm sahəsində tədqiqat fəaliyyətinin əksəriyyəti elmi-tədqiqatları dəstəkləmək üçün hesablama alətlərinin və infrastrukturun yaradılmasına yönəlib [7]. E-elm infrastrukturunu paylanmış hesablama texnologiyalarından geniş istifadə etməklə elmi-tədqiqatlar aparmağa imkan verir və superkompüter resursları, yüksək sürətli şəbəkələr, qrid infrastrukturunu, verilənlər saxlanıcı və birgə istifadə edilən digər resurslar daxildir. Bu infrastruktur alimlərə texniki resurslardan birgə, əlaqələndirilmiş şəkildə və asanlıqla istifadə etməyə imkan verir. E-elm infrastrukturunun tərkib hissələri unikal elmi-tədqiqat alətləri – fəvqəlgüclü elektron mikroskoplar,

elementar zərrəciklərin sürətləndiriciləri, mürəkkəb tibbi avadanlıq və s. ola bilər.

III. E-ELMİN TEXNOLOJİ İNFRASTRUKTURU

Qrid infrastrukturunu e-elm üçün əsas infrastruktur hesab edilir, e-elm məsələlərinin reallaşdırılması üçün ilk və əsas çıxışı qrid texnologiyaları açmışdır. Müasir elmi-tədqiqatlarda nəhəng həcmdə informasiya istifadə edilir (məsələn, böyük adron kolları ildə 25 Pbayt informasiya generasiya edir) və hazırda belə axınların saxlanması və emalı üçün yeganə həll qriddir.

Qrid paylanmış, dinamik virtual təşkilatlarda müxtəlif resursların ortaq və əlaqələndirilmiş istifadəsini dəstəkləyən texnologiyalar və infraqurudur [8]. Qrid bütün əhəmiyyətli resurslara çevik, yüksək sürətli girişi təmin edir, tələbata görə virtual hesablama sistemi yaratmağa imkan verir. Qrid yüksək sürətli kompüterləri, böyük məlumat bazalarını, tədqiqat avadanlığını, proqram təminatını, tədqiqatçıları şəbəkə vasitəsilə əlaqələndirməyə xidmət edən əsas texnologiya və idarəetmə sistemidir. Qridi hesablama qridi, verilənlər qridi və giriş qridi (ing. access grid) kimi siniflərə bölmək olar [8]. Hesablama qridi paylanmış birgə hesablama resursları (metakompüter resursları) yaradır, olduqca böyük miqyaslı, yüksək sürətli hesablama və məsafədən nəzarət imkanı verir. Verilənlər qridi coğrafi paylanmış böyük miqyaslı verilənlərin analizini və idarə olunmasını, yüksək sürətli İnternetdən istifadə etməklə beynəlxalq əməkdaşlığı həyata keçirtməyə xidmət edir. Giriş qridi birgə əməkdaşlığı dəstəkləmək üçün interfeys təqdim edir, real vaxtda məsafədən konfranslara və qrid infrastrukturunda birgə tədqiqatlara imkan verir.

İnkişaf etmiş ölkələrdə qrid infrastrukturunun yaradılması üzrə 2000-ci illərdə 40-a yaxın layihə həyata keçirilmişdir [9]: ABŞ-da 4 iri superkompüter mərkəzlərinin resurslarının birləşdirilməsi üzrə TeraGrid (2000-2007), böyük hesablama gücləri tələb edən elmi tədqiqatların aparılması üçün Open Science Grid, Avropada 18 kompüter mərkəzini birləşdirən DEISA (Distributed European Infrastructure for Supercomputing Applications), Avropa İttifaqında yüksək enerjilər, ekologiya və bioinformatika sahəsində verilənlərin emalı üçün qridin qurulması üzrə DataGrid (1998-2007) layihələri, Yaponiyada elmi-tədqiqat fəaliyyəti üçün qrid infrastrukturunun qurulması üzrə NAREGI (National Research Grid Initiative) layihəsi (2003-2007) və s. Avropa İttifaqı tərəfindən maliyyələşdirilən EGEE (Enabling Grids for E-science, "E-elm üçün qridlərin inkişaf etdirilməsi") layihəsinin məqsədi qrid-texnologiyaların ən son nailiyyətlərindən istifadə edərək elmi-tədqiqatlar üçün tətbiqi qrid-servisler infrastrukturunu yaratmaq idi. EGEE layihəsi üç mərhələdə - EGEE (2004, aprel-2006, mart), EGEE II (aprel 2006 -2008, aprel), EGEE III (2008, may-2010) həyata keçirilmişdir (xələfi EGI – European Grid Initiative layihəsidir).

Məlumdur ki, qrid-sistem üç əsas elementə əsaslanır: hesablama resursları (klasterlər), resursların İnternetə yüksək sürətlə və etibarlı çıxışı və bu resursları vahid hesablama kompleksində birləşdirən aralıq proqram təminatı (ing. middleware). Aralıq proqram təminatı yüksək sürətli şəbəkələrlə, kompüter klasterləri, yaddaş serverlərindən təşkil olunan paylanmış qridin baza infrastrukturunu üzərində yaradılır.

Onun sayəsində müxtəlif təşkilatların domenlər çoxluğunda iş vahid qrid-mühitindəki kimi aparılır, istifadəçilərə vahid resurs kimi təqdim olunur.

Qrid infrastrukturunun yaradılması üçün gLite (EGEE çərçivəsində yaradılmışdır), Legion, UNICORE (UNiform Interface to COmputing RESources), Globus Toolkit, ARC (Advanced Resource Connector) və s. kimi bir sıra proqram təminatı paketləri mövcuddur. Açıq kodlu proqram təminatı olan Globus Toolkit paketi bu sahədə de facto standart hesab edilir [10]. Globus Toolkit qrid infrastrukturunun qurulması üçün baza vasitələri təqdim edir (tapşırıqların idarə edilməsi, monitorinqi və koordinasiyası, paylanmış verilənlərə müraciət edilməsi, faylların ötürülməsi, informasiya xidmətləri və təhlükəsizlik).

IV. İSTİFADƏÇİLƏRİN İDENTİFİKASIYASI SİSTEMLƏRİ

E-elm müxtəlif inzibati domenlərdən ibarətdir, onların hər birinin öz avtonom informasiya təhlükəsizliyi mexanizmləri var. Effektiv təhlükəsizlik arxitekturu elə protokollar təqdim etməlidir ki, onlar avtonom mexanizmlər arasındakı fərqləri kompensasiya etməyə imkan versinlər, eyni zamanda hər bir lokal qovşağın ona aid olan resurslara tam nəzarət etməsini təmin etsinlər. İnternetə informasiya təhlükəsizliyi istifadəçilərə və provayderlərə rahat şəkildə təmin edilməlidir, bu baxımdan e-elm infrastrukturunda vahid giriş servisinin təmin edilməsi vacibdir. Vahid giriş dedikdə istifadəçilərin autentifikasiya proseduru yalnız bir dəfə keçməsi nəzərdə tutulur, bundan sonra onun istifadə edəcəyi bütün resurslarda autentifikasiyasını sistem öz üzərinə götürür.

Paylanmış resurslara giriş problemini qarşılıqlı əlaqəli iki problemə ayırmaq olar: 1) təşkilatların və istifadəçilərin federasiyalarının dəstəklənməsi; 2) federasiyalara daxil olan təşkilatların resurslarına istifadəçilərin qarşılıqlı girişlərinin təmin edilməsi.

Federasiya istifadəçi atributlarının və identifikasiya məlumatlarının müəyyən siyasət əsasında müxtəlif domenlər arasında paylanmasını həyata keçirən modeldir.

Federativ modelin iki əsas komponenti var:

- İdentifikasiya Provayderi (IdP) – istifadəçilərin autentifikasiyasını həyata keçirir və identifikasiya məlumatlarını idarə edir.
- Servis provayderi (SP) – istifadəçilərə servislər göstərir, istifadəçinin etibarlı olduğunu IdP-nin autentifikasiya məlumatlarına əsasən yoxlayır.

Birinci problem təşkilatlarda mövcud olan istifadəçiləri identifikasiya sistemləri (IdP) arasında inam münasibətlərinin yaradılması yolu ilə həyata keçirilir. Belə IdP federasiyaları onlara daxil olan təşkilatın istifadəçisi başqa təşkilatın resurslarına müraciət etdikdə məsafədən autentifikasiyanı həyata keçirməyə imkan verir. Bundan başqa, IdP federasiyaları istifadəçilərin atributları haqqında məlumat mübadiləsinə də şərait yaradır ki, bunlar da istifadəçinin giriş səviyyəsini, istifadəçiyə icazə verilən resursların və servislərin kateqoriyalarını müəyyən etməyə imkan verir.

E-elm şəbəkəsində IdP federasiyaları infrastrukturunu yaratmaq üçün iki əsas platforma: Shibboleth və A-Select istifadə edilir, hər iki platforma pulsuz yayılır. IdP federasiyaları geniş istifadə olunan açıq açarlar infrastrukturuna (Public Key Infrastructure, PKI) əsaslanır. İstifadəçilərin və resursların identifikatorları kimi X.509 rəqəmsal sertifikatları istifadə edilir [11]. Federativ autentifikasiya və avtorizasiya infrastrukturunun (AAI) yaradılması Avropa elmi-tədqiqat şəbəkələrinin ən vacib təşəbbüslərindən biridir. Hazırda həyata keçirilən eduGAIN layihəsi öz qarşısına GEANT şəbəkəsində federativ AAI yaradılması məqsədini qoymuşdur.

İkinci problem – paylanmış federativ resurslara giriş virtual təşkilatlar vasitəsi ilə dəstəklənir. E-elm mühitində tərəflər dinamik olaraq virtual təşkilatlar formalaşdırırlar və bu virtual təşkilatlar arasında inam münasibətlərinin yaradılması sadə məsələ deyil. Virtual təşkilatlar inam münasibətlərini çox vaxt mərkəzi avtorizasiya serveri (Community Authorization Service, CAS) vasitəsi ilə həyata keçirməyə üstünlük verirlər. Resurs təklif edən hər bir tərəf bu resursa giriş zamanı virtual təşkilat üzvlərinin nəzərə alınmalı olduqları hüquqlar bərsində CAS serverini məlumatlandırır. Resursa müraciət etmək üçün istifadəçi öz imtiyazlarını nəzərə alınmaqla CAS serverindən müvafiq sertifikat alır. Bu sertifikat resursa təqdim edilir və resurs mandatı (credential) yoxladıqdan sonra girişə icazə verir. Bir neçə virtual təşkilata daxil olan istifadəçi bir neçə müvafiq mandatdan istifadə etməlidir ki, bu da istifadəçi üçün müəyyən çətinlik yaradır.

NƏTİCƏ

Qloballaşan dünyada elm və texnologiya sahəsində yüksək rəqabət qabiliyyətini təmin etmək üçün ölkələr e-elm infrastrukturunun qurulmasına cəhd edirlər. Paylanmış, heterogen, əksər hallarda müxtəlif ölkələrin ərazisinə səpələnmiş bu infrastrukturda ən vacib məsələlərdən biri də istifadəçilərin etibarlı identifikasiyasını təmin etməkdir.

Təqdim olunan işdə e-elm mühitində istifadəçilərin identifikasiyası modelləri analiz edilir, onların üstün və çatışmayan cəhətləri müəyyən edilir.

ƏDƏBİYYAT

- [1] “Azərbaycan Respublikasında 2009–2015-ci illərdə elmin inkişafı üzrə Milli Strategiya”nın və “Azərbaycan Respublikasında 2009–2015-ci illərdə elmin inkişafı üzrə Milli Strategiyanın həyata keçirilməsi ilə bağlı Dövlət Proqramı”nın təsdiq edilməsi haqqında AR Prezidentinin sərəncamı, 4 may 2009-cu il.
- [2] İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı. 26 sentyabr 2012-ci il.
- [3] Nentwich M., Cyberscience: Research in the age of the Internet. Vienna: Austrian Academy of Sciences Press. 2003.
- [4] Паринов С.И., e-Science - онлайнное будущее науки // Приложение к журналу Информационные технологии, 2007, №9, с.1-32.
- [5] NSF, Cyberinfrastructure vision for 21st century discovery, National Science Foundation Cyberinfrastructure Council, March 2007, NSF07-28.
- [6] National e-Science Centre definition of e-Science. <http://www.nesc.ac.uk/nesc/define.html>
- [7] Jankowski N.W., Exploring e-science: An introduction // Journal of Computer-Mediated Communication, 2007, Vol. 12, No. 2, pp. 549-562.
- [8] Foster I., The Grid: A New Infrastructure for 21st Century Science // Physics Today, 2002, Vol. 55, No. 2, pp. 42-47.
- [9] Riedel M. et al. Interoperation of World-Wide Production e-Science Infrastructures // Concurrency and Computation: Practice and Experience, 2008, Vol.21, No.8, pp.961-990.
- [10] Globus Grid Project <http://www.globus.org>.
- [11] Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W., Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL), RFC 5280, 2008, 151 p.