UOT 004.056

***Əliquliyev R.M.*[1], *Abdullayeva F.C.*[2]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]director@iit.ab.az , [2]farqana@iit.ab.az

BULUD TEXNOLOGİYALARINDA İNAM MƏSƏLƏLƏRİNİN ANALİZİ

Təqdim olunan işdə bulud texnologiyalarının təhlükəsizlik problemləri sırasında mühüm məsələ olan inam məsələləri araşdırılır. Bunun üçün müxtəlif elm sahələri tərəfindən öyrənilmiş inam anlayışına aydınlıq gətirilir, bulud texnologiyaları üçün aktual olan reputasiya tipli inamın yaradılması texnologiyaları, buludların şəffaflığının təmin edilməsinə yanaşmalar, inamın servis səviyyəsi müqaviləsinə əsasən qurulması üsulları, "inam servis kimi" xidmətləri araşdırılır. Göstərilən inam mexanizmlərində mövcud problemlər müəyyən olunur və onların həlli üçün bir sıra tövsiyələr verilir.

Açar sözlər: *Bulud texnologiyaları, inam, servis səviyyəsi müqaviləsi, reputasiya tipli inam, Sibil hücumları.*

Giriş

Bulud texnologiyaları informasiya kommunikasiya texnologiyaları (İKT) sahəsində mühüm əhəmiyyətə malik perspektivli bir texnologiyadır. Bulud texnologiyalarının təyinatı hər hansı kənar təşkilatın infrastrukturunda yerləşmiş məlumat mərkəzlərindən istifadəçilərə İnternet vasitəsilə dinamik xarakterli, çevik və birgə istifadə üçün nəzərdə tutulmuş resurslar (yaddaş, proqram təminatı və s.) təqdim etməkdir. Lakin bulud texnologiyalarının son dərəcə paylanmış və qeyri-şəffaf təbiətə malik olması onun texnologiyalar bazarında uğur qazanmasına əhəmiyyətli dərəcədə manea törədir [1]. Bulud texnologiyalarının geniş yayılmasına mane olan problemlər sırasında mühüm əhəmiyyət daşıyan məsələlərdən biri də inam məsələləridir [2, 3].

Bulud mühitində inam münasibətlərinin qurulmasına xidmət edən çox sayda yanaşmalar irəli sürülmüşdür [4, 5]. Lakin mövcud yanaşmalarda qiymətləndirmə üçün lazım olan məlumatı əlaqədar mərkəzlərə bulud provayderlərinin özləri təqdim edirlər. Burada bəzi bulud provayderlərinin məlumatı filtrasiya etdikdən və ya dəyişdirdikdən sonra təqdim etməsi ehtimalı çox böyükdür. Bu isə inam qərarının qəbulunda məlumatın doğruluğunu şübhə altına qoyur.

Təqdim olunan işdə bulud texnologiyalarında reputasiya tipli inamın yaradılması üsullarının, buludların şəffaflığının təmin edilməsinə yanaşmaların, inamın servis səviyyəsi müqaviləsinə əsasən qurulması üsullarının, "inam servis kimi" xidmətlərinin analizi aparılır. Provayderin inam səviyyəsini düzgün qiymətləndirmək üçün inam göstəricilərinin yoxlanmasının üçüncü tərəf peşəkar təşkilatlar tərəfindən avtomatik olaraq həyata keçirilməsi tövsiyə olunur.

İnam anlayışı

Ümumiyyətlə, *inam* sosial-psixologiya, sosiologiya, iqtisadiyyat, marketinq kimi müxtəlif elmlər tərəfindən öyrənilən çoxşaxəli anlayışdır [6]. Bu anlayışın geniş araşdırılmasına baxmayaraq, hazırkı dövrədək ona standart tərif verilməmişdir və ayrı-ayrı mənbələrdə inam bir-birindən fərqli şərh olunur [7–11]. Məsələn, Y. Wang və J. Vassileva inama aşağıdakı kimi tərif verirlər:

İnam (ing., trust) – bir subyektin özünün bilavasitə təəssüratlarına əsaslanaraq digər subyektin imkanlarına, düzgünlüyünə və etibarlılığına olan güvənidir [11].

Bu inam anlayışının sosioloji tərifidir. Lakin bulud texnologiyalarında inam məsələlərinə həsr olunmuş mənbələrdə inam termini əksər hallarda informasiya təhlükəsizliyi (ing., security) və gizlilik (ing., privacy) baxımından istifadə olunur [12].

Ümumiyyətlə, bulud texnologiyaları meydana gəldiyi dövrdən (2007-ci il) bu texnologiyaya istifadəçilərin inamı çox aşağı idi [13]. Belə ki, Fujitsu Elmi Tədqiqat İnstitutunun

2010-cu ildə 6 ölkə üzrə 3000-dən çox bulud müştərisi arasında aparılan sorğu əsasında tərtib etdiyi analitik materialda müştərilərin buludlara inamının olmamasının səbəbləri verilmişdir. Burada göstərilir ki, müştərilərin 88%-i fərdi məlumatlara kimlərin giriş əldə edəcəyinə əmin olmadıqları üçün, 84%-i isə fərdi məlumatların saxlanacağı məkandan narahat olduğu üçün buludlara inanmır [13].

Lakin hazırda bulud bazarına nəzər saldıqda görünür ki, son zamanlar bulud texnologiyalarının tətbiq dinamikasında kəskin artım müşahidə olunur [14]. Gartner analitik təşkilatı bulud bazarındakı gəlirlərin 2010-cu ildə 77 milyard dollardan 2016-cı ildə 210 milyard dollara dəyişəcəyini proqnozlaşdırır. Qeyd olunur ki, bu gəlirin 41,3%-i "İnfrastruktur servis kimi" bulud xidmətinin hesabına əldə olunacaqdır. Bundan əlavə, 2016-cı ilin sonlarında dünyanın 1000 ən böyük təşkilatının 50 faizi öz həssas müştəri məlumatlarını ümumi bulud infrastrukturunda yerləşdirəcəyini planlaşdırır. Digər tərəfdən, Market Research Media Ltd təşkilatı tərəfindən CAGR (Compound Annual Growth Rate) kalkulyatoru vasitəsilə bulud bazarının 2015-2020-ci illərdə gəliri 270 milyard dollar həcmində qiymətləndirilmişdir [15]. CAGR (mürəkkəb illik artım tempi) – investisiyaların artım tempini zamana görə hesablayan kalkulyatordur.

Hazırda bulud provayderlərinin inam dərəcəsini müəyyən etməyə xidmət edən çox sayda inam mexanizmləri yaradılmışdır. Aşağıda onların əsas siniflərinin qısa xülasəsi verilir.

Buludlarda şəffaflığın təmin edilməsi

Buludların inam dərəcəsinin müəyyən edilməsinin ən vacib məsələlərindən biri buludların şəffaflığının təmin edilməsidir. Heç bir bulud şəffaflıq xüsusiyyətinə malik deyil [16]. Yəni, buludlarda nə istifadə olunan texnologiyaları, nə də orada gedən prosesləri görmək mümkün deyil. Şəffaflıq bulud provayderlərinin inam qazanmasına təsir edən əsas faktor kimi qiymətləndirilir [5]. Şəffaflıq olmadan, inam yaratmaq mümkün deyil.

Bulud texnologiyalarında şəffaflıq və cavabdehlik problemlərinin həlli hər zaman beynəlxalq təşkilatların diqqət mərkəzində olmuşdur. Belə ki, buludların şəffaflığını müəyyən etmək üçün bu sahədə aparıcı təşkilatları birləşdirən Bulud Təhlükəsizliyi Alyansı (Cloud Security Alliance, CSA) 2011-ci ilin sonlarında "Təhlükəsizlik, İnam və Zəmanət Reyestri" (Security, Trust & Assurance Registry, STAR) [17] adlı proqram hazırlamışdır. Reyestri CSA təşkilatının saytından pulsuz əldə etmək mümkündür. Bu reyestr provayderlərin təhlükəsizlik səviyyəsinin özünüqiymətləndirmə mexanizmlərinə əsaslanır və iki sənəddən ibarətdir:

1. Servis provayderinin təhlükəsizlik tələblərinə uyğunluğunun attestasiya anketi (Consensus Assessments Initiative Questionnaire, CAIQ). CAIQ elektron cədvəl şəklində hazırlanmış sənəddir, bulud provayderinin hə/yox formatında cavablandıracağı suallar çoxluğundan ibarətdir.
2. Bulud İdarəetmə Matrisi (Cloud Controls Matrix, CCM). CCM bulud provayderinin təhlükəsizlik səviyyəsini müəyyən edən ümumi prinsiplərdən ibarət sənəddir. O, bulud provayderinin CSA-nın 13 bənddən ibarət hazırladığı təhlükəsizlik təlimatının [18] tələblərinə nə dərəcədə cavab verdiyini müəyyən edir.

CSA təşkilatının verdiyi məlumata görə, öz şəffaflığını müəyyən etmək üçün indiyədək 30-dan çox qabaqcıl bulud provayderi özlərinin STAR sənədini tərtib etmişdir. Bu provayderlər sırasına Google, Microsoft, Verizon, Intel, McAfee və s. aid edilir.

İnamın qurulmasına xidmət edən mexanizmlərdən biri də 2009-cu ildə CSC (Computer Sciences Corporation) təşkilatı tərəfindən təklif edilən CTP (Cloud Trust Protocol) protokoludur [16]. Protokol sorğu-cavab mexanizminə əsaslanır. Burada istifadəçilər provayderin şəffaflıq elementləri haqqında konkret məlumat əldə etmək üçün provayderə müvafiq sorğu göndərməklə cavab əldə edirlər. Şəffaflıq elementlərinə bulud infrastrukturunun konfiqurasiyası, boşluqları, audit hesabları, servisin idarə edilməsi mexanizmləri və s. kimi elementlər daxildir. Protokolun bulud mühitində reallaşdırılmasını CSA təşkilatı öz üzərinə götürmüşdür və onu 2011–ci ildə

özünün GRC (Governance, Risk Management and Compliance) adlı sənədlər toplusuna əlavə etmişdir. Protokolun məqsədi istifadəçilərin bulud infrastrukturunda baş verən hadisələr haqqında məlumat əldə etməsinə şərait yaratmaqdır. CTP istifadəçilərin buludda baş verən hadisələri sanki daxildən izləməsinə şərait yaradaraq, bulud istifadəçiləri ilə bulud provayderləri arasında ötürücü vasitə rolunda çıxış edir.

Servis səviyyəsi müqaviləsi

Bulud texnologiyalarında inam münasibətlərinin qurulmasına yanaşmalardan biri də Servis Səviyyəsi Müqaviləsidir (Service Level Agreement, SLA). SLA – servis provayderi ilə müştəri arasında bağlanan müqavilədir, provayderin iddia etdiyi servis keyfiyyətinə (Quality of Service, QoS) zəmanəti təmin edir və müqavilənin şərtlərinin pozulması halları baş verdikdə, subyektə hüquq müstəvisində cərimə tətbiq olunmasına şərait yaradır [19]. SLA bir çox indikatorlardan ibarət olur. SLA indikatorlarına əlyetərlik (fasiləsiz işləmə müddəti və fasilələrlə işləmə müddəti), cavab vermə vaxtı, çeviklik və s. parametrlər və ya məhdudiyyətlər aid edilir.

Servis provayderləri (SP) xidmətlər göstərdikdə bu indikatorlara riayət etmək məcburiyyətində olur. Bu indikatorların hər hansı birində yol verilən pozuntular SP-nin cərimələnməsi, həmçinin müştəridə SP-nə qarşı mənfi rəyin formalaşması ilə nəticələnə bilər.

Hazırda dünyada bulud xidmətləri göstərən əksər böyük təşkilatlar SLA-ya uyğun xidmətlər göstərməyə cəhd edir. Məsələn, bulud xidmətləri göstərən 3Tera təşkilatının məlumat mərkəzinin təqdim etdiyi servislərin SLA səviyyəsi "beş ədəd doqquz" təşkil edir. Yəni 3Tera servisləri SLA-da göstərdiyi tələblərə 99,999% faiz əməl edərək təqdim etdiyini bəyan edir. Burada göstərilən xidmətlərin səviyyəsi 99,999% faizdən aşağı düşdüyü halda müştərinin hesabına kompensasiya ödənilməsi şərti qoyulur. Başqa halda, Amazon təşkilatının EC2 (Elastic Compute Cloud) servisi üçün elan etdiyi SLA-nın faiz dərəcəsi 99,95% təşkil edir. Burada da SLA-nın faiz dərəcəsi vəd ediləndən aşağı təşkil etdiyi halda Amazon təşkilatı da müştərilərə kompensasiya ödəyir. Lakin istifadəçilərin kompensasiya alması üçün onlar servisin göstərilməsində fasilələri əks etdirən faktları sənədli şəkildə Amazon şirkətinə təqdim etməlidir.

Adətən, SLA-ya əsasən qurulan inam modelləri bu müqavilədə vəd edilən göstəricilərin monitorinqinin aparılması məsələlərinə həsr olunur [20, 21]. Belə monitorinq sistemlərinə misal olaraq wiSLA, Traverse, IT SLA monitoring sistemlərini göstərmək olar.

İnam servis kimi

Buludların inam dərəcəsini müəyyən edən mexanizmlərdən biri də "İnam servis kimi" (Trust as a Service, TaaS) xidmətlərinin göstərilməsidir.

TaaS – təhlükəsizlik xidmətlərinin servis provayderi ilə heç bir əlaqəsi olmayan inanılmış üçüncü şəxs tərəfindən sorğu əsasında təqdim olunmasıdır. Bu mexanizmlərdən biri olan Cloud Trust Authority (CTA) EMC təşkilatının RSA bölməsi tərəfindən 2011-ci ildə təklif edilmişdir. CTA müxtəlif provayderlərin təqdim etdiyi servislərin təhlükəsizliyinin idarə edilməsində vahid mərkəz funksiyasını yerinə yetirir. CTA-nın tərkibinə daxil olan identifikasiyanın idarə edilməsi bloku müxtəlif bulud provayderləri arasında vahid girişin təmin edilməsini həyata keçirir.

Digər tərəfdən, burada normativ sənədlərə riayət bloku kənar istifadəçilərə imkan verir ki, onlar servis provayderinin müəyyən etalona nəzərən formalaşmış təhlükəsizlik profilini izləyə bilsin. RSA-nın inamın formalaşdırılmasında fəlsəfəsi şəffaflıq və idarəetmə mexanizmlərini sintez etməkdən ibarətdir və adətən, o inamı "İnam = Şəffaflıq + İdarəetmə" kimi müəyyən edir [22].

Reputasiya tipli inam

Hazırda buludların reputasiya tipli inam məsələlərinə də böyük diqqət yetirilir. İnam anlayışında olduğu kimi, reputasiya anlayışı da müxtəlif elm istiqamətlərində dərindən araşdırılmışdır, lakin hələ də bu anlayışa da standart tərif formalaşmamışdır [23–26]. Ayrı-ayrı mənbələrdə reputasiya anlayışı müxtəlif formada şərh olunur [1, 27, 28]. Belə ki, mənbə [11]-də reputasiyaya verilən tərif aşağıdakı kimidir:

Reputasiya – bir subyektin başqa subyektlərdən aldığı tövsiyələr əsasında digər subyektin imkanlarına, düzgünlüyünə və etibarlılığına olan güvənidir [11].

Reputasiya sistemləri – bir cəmiyyətin ayrı-ayrı üzvlərinin konkret obyektə (məsələn, servis provayderləri, servislər, subyektlər) verdiyi rəylər əsasında obyekt üçün reputasiya xalları hesablamağa xidmət edir [29].

İnam və reputasiya anlayışları müxtəlif tətbiq sahələrinə malikdirlər, lakin bir-biri ilə sıx əlaqəli anlayışlardır. Bu anlayışların hər ikisi subyektin güvənlilik dərəcəsini qiymətləndirmək üçün istifadə olunur [11]. Lakin bunları fərqləndirən cəhət odur ki, inam iki subyekt arasında qurulan münasibətdir, subyektin reputasiyası isə cəmiyyətin həmin subyektə qarşı olan ümumi rəyidir.

Adətən, cəmiyyətin çox sayda subyekti tərəfindən inam qazanmış subyekt yüksək reputasiyaya malik olur. Bulud mühitində inam subyekti üzərində inam qərarı qəbul etmək istəyən subyekt inam subyektinin inam səviyyəsini bu reputasiya əsasında qiymətləndirir.

Ümumiyyətlə, müxtəlif mənbələrdə reputasiya sistemlərindən savayı, "tövsiyə sistemləri" terminə də rast gəlmək mümkündür. Bu sistemlər arasında fərq ondan ibarətdir ki, reputasiya sistemləri yalnız bir cəmiyyətdə toplanmış iştirakçıların rəyinə əsaslanır, tövsiyə sistemləri isə kənardan verilən rəyləri də nəzərə alır.

Məşhur reputasiya sistemləri sırasına Truster, TrustedSource sistemlərini aid etmək olar. Hazırda bir çox veb-saytlar Slashdot, Reddit, Digg, eBay və s. reputasiya sistemlərindən istifadə edir. Müxtəlif alış-veriş saytlarında alıcı və satıcılar hər dəfə alış-veriş etdikdən sonra bir-birini qiymətləndirirlər.

Konkret satıcı (alıcı) ilə bağlı reytinqlər (qiymətlər) həmin veb-saytın (məsələn, eBay) reputasiya sistemi tərəfindən hesablanır və alınan ədəd satıcının (alıcının) inam dərəcəsini göstərir. Reputasiya sistemləri İnternet təhlükəsizliyində də geniş istifadə olunur. Bu növ sistemlərdən ən məşhuru TrustedSource sistemidir.

TrustedSource sistemi CipherTrust qurumu tərəfindən yaradılmışdır və hazırda McAfee şirkətinə məxsusdur. İnternet identifikasiyaları (məsələn, İP-ünvan, domenlər, poçt kontenti, veb-kontent) üçün reputasiya xalları hesablamağa xidmət edir. TrustedSource hər bir İnternet identifikasiyanın bədlik dərəcəsini Data Mining və digər analiz üsullarından istifadə edərək müəyyən edir. Ümumiyyətlə, İnternet reputasiya sistemləri e-poçt, veb və bir sıra protokollarla ötürülən şəbəkə hücumlarının qarşısını almaqda faydalı vasitədir.

Digər tətbiq sahələrinə aid reputasiya sistemlərinə aşağıdakıları misal göstərmək olar: P2P sistemlərində – etibarlı qovşaqların müəyyən edilməsi, sosial xəbərlərdə–ən yaxşı xəbərin müəyyən edilməsi, veb-axtarış sistemlərində–PageRank [29].

Reputasiya sistemləri bir sıra hücumlara qarşı olduqca zəifdir. ENİSA təşkilatı bu sistemlər üçün aktual olan 15 hücum növünü müəyyən etmişdir [30]. Bu hücumlar sırasında bulud infrastrukturu üçün aktual olanı Sibil hücumudur (Sybil attack) [31].

Sibil hücumunu bəzən psevdospufinq (ing., pseudospoofing) də adlandırırlar. Burada hücum edən çox sayda identifikator (sibil) yaradaraq, onları subyektin reputasiya xalını manipulyasiya etmək məqsədilə istifadə edir.

İlk dəfə Sybil adı 1973-cü ildə ingilis jurnalisti Flora Şreyberin «Sybil» kitabında [32] işlədilmişdir. Bu kitab psixiatrik klinikanın xəstəsi olan Shirley Ardell Masonun həyatından bəhs edir. Burada Sybil Isabel Dorsett adı Masonun adının məxfiliyinin qorunması üçün istifadə edilmişdir. Süjetin mahiyyətinə görə Sybil identikliyin dissosiativ sarsılması

xəstəliyindən əziyyət çəkir. Bu xəstəlik bir şəxsin vücudunda bir neçə ayrı-ayrı şəxsin formalaşması ilə xarakterizə olunur. Psixoloqla müsahibədən sonra məlum olur ki, Sybil Dorsettin vücudunda 16 müxtəlif şəxs cəmləşir. Yeri gəldikcə o, özünü cəmiyyətə bu şəxslərin adı altında təqdim edir.

İnformasiya sistemlərində çoxsaylı identifikasiyaların saxtalaşdırılmasını ilk dəfə Sybil hücumu adlandıran John R. Douceur [33] olmuşdur.

Nəticə

Bulud provayderlərinin inam dərəcəsini müəyyən etməyə imkan verən mexanizmlərin çatışmazlığı qiymətləndirmə üçün lazım olan məlumatı əlaqədar mərkəzlərə bulud provayderlərinin özlərinin təqdim etməsidir. Burada bəzi bulud provayderlərinin məlumatı filtrasiya etdikdən və ya dəyişdirdikdən sonra təqdim etməsi ehtimalı çox böyükdür. Bu isə inam qərarının qəbulunda məlumatın doğruluğunu şübhə altına qoyur. Odur ki, bulud mühitində yuxarıda sadalanan inam göstəricilərinin yoxlanması üçüncü tərəf peşəkar təşkilatlar tərəfindən avtomatik olaraq həyata keçirilsə, provayderin inam səviyyəsini düzgün qiymətləndirmək mümkün olar. Bu isə bulud texnologiyalarının geniş istifadəsi üçün şərait yarada bilər. Digər tərəfdən, Sibil hücumlarına davamlı olan reputasiya sistemlərinin yaradılması bulud texnologiyalarının geniş tətbiqi üçün zəmin yarada bilər.

Ədəbiyyat

1. Habib S.M., Hauke S., Ries S., Muhlh M. Trust as a facilitator in cloud computing: a survey // Journal of Cloud Computing: Advances, Systems and Applications, 2012, vol. 1, no 19, 33 p.
2. Alguliev R.M., Abdullayeva F.C. Identity management based security architecture of cloud computing on multi-agent systems / Proc. of the Third International Conference on Innovative Computing Technology (INTECH), 2013, pp. 123–126.
3. Əliquliyev R.M., Abdullayeva F.C. Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya Texnologiyaları Problemləri, 2013, №1, s. 3–14.
4. Rashidi A., Movahhedinia N. A model for user trust in cloud computing // International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2012, vol. 2, no. 2, pp. 1–8.
5. Huang J., Nicol D.M. Trust mechanisms for cloud computing // Journal of Cloud Computing: Advances, Systems and Applications, 2013, vol. 2, no 9, 14 p.
6. Heijden V.H., Verhagen T., Creemers M., Creemers M. Understanding online purchase intentions: contributions from technology and trust perspectives // European Journal of Information Systems, 2003, vol. 12, no 1, pp. 41–48.
7. Castelfranchi C., Falcone R. Principles of trust for MAS: Cognitive anatomy social importance, and quantication / Proc. of the IEEE Third International Conference on Multi-Agent Systems, 1998, pp. 72–79.
8. Gambetta D. Can we trust trust? Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 1990, Chapter 13, pp. 213–237.
9. Montaner M., Lopez B., Rosa J.L. Opinion-based filtering through trust / Proc. of the 6th International Workshop on Cooperative Information Agents VI, 2002, pp. 164–178.
10. Jøsang A., Ismail R., Boyd C. A survey of trust and reputation systems for online service provision // Journal of Decision Support Systems, vol. 43, no 2, pp.618–644.
11. Wang Y., Vassileva J. Trust and reputation model in peer-to-peer networks / Proc. of IEEE Conference on P2P Computing, 2003, pp. 1–8.
12. Ghosh A., Arce I. Guest editors' introduction: In Cloud Computing We Trust–But Should We? // IEEE Security & Privacy, 2010, vol. 8, no 6, pp. 14–16.
13. Personal data in the cloud: A global survey of consumer attitudes. Fujitsu Research Institute, 2010, Japan, 23 p.

14. Columbus L. Gartner predicts infrastructure services will accelerate cloud computing Growth. http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.
15. Global cloud computing market forecast 2015-2020. Market Research Media Ltd, http://www.marketresearchmedia.com/?p=839.
16. Knode R. Digital trust in the cloud: Liquid security in cloudy places, CSC.COM, 2009, 40 p.
17. Security, Trust and Assurance Registry (STAR). Cloud Security Alliance (CSA), 2011, https://cloudsecurityalliance.org/star/.
18. Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance (CSA), 2011, v.3.0, 176 p.
19. Haq I.U., Brandic I., Schikuta E. SLA validation in layered cloud infrastructures / Proc. of the 7th International Conference on Economics of Grids, Clouds, Systems, and Services, 2010, pp. 153–164.
20. Wang S.X., Zhang L., Wang S., Qiu X. A cloud-based trust model for evaluating quality of web services // Journal of Computer Science and Technology, 2010, vol. 25, no 6, pp. 1130–1142.
21. Wieder P., Yahyapour R., Ziegler W. Grids and Service-Oriented Architectures for Service Level Agreements, Springer, 2010, chapter 5, 171 p.
22. EMC's vision for trust in the cloud. Proof, not promises: Creating the trusted cloud, EMC Corporation, 2011, 15 p.
23. Zacharia G., Moukas A., Maes P. Collaborative reputation mechanisms in electronic marketplaces // Decision Support Systems, , 2000, vol. 29, no 4, pp. 371–388.
24. Yu B., Singh P.M. An evidential model of distributed reputation management / Proc. of the First International Joint Conference on Autonomous Agents and Multiagent Systems, 2002, pp. 294–301.
25. Yu B., Singh P.M. A social mechanism of reputation management in electronic communities /Proc. of Fourth International Workshop on Cooperative Information Agents, 2000, pp. 154–165.
26. Schafer B.J., Konstan J., Riedl J. Recommender systems in e-commerce / ACM Conference on Electronic Commerce, 1999, pp. 158–166.
27. Chang E., Dillon T.S., Hussain F.K. Trust and reputation relationships in service-oriented environments / Proc. of the Third International Conference on Information Technology and Applications (ICITA), 2005, vol. 1, pp. 4–14.
28. Wang S.X., Zhang L., Wang S. Qiu X. A cloud-based trust model for evaluating quality of Web services // Journal of Computer Science And Technology, 2010, vol. 25, no 6, pp. 1130–1142.
29. Reputation system. From Wikipedia, the free encyclopedia / http://en.wikipedia.org/wiki/Reputation_system.
30. Carrara E., Hogben G. Reputation-based systems: a security analysis. ENISA Position Paper, 2007, no 2, 32 p.
31. Talal H.N., Quan Z.S., Sheng A.A. Reputation attacks detection for effective trust assessment among cloud services / Proc. of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 469–476.
32. Schreiber F.R. Sybil. Warner Books, 1973, 359 p.
33. Douceur J.R. The Sybil Attack / Proc. of 1st International Workshop on Peer-to-Peer Systems (IPTPS), 2002, pp. 1–6.

УДК 004.056

Алгулиев Расим М.[1], Абдуллаева Фаргана Д.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]director@iit.ab.az, [2]farqana@iit.ab.az

Исследование проблем доверия в облачных технологиях

В статье исследуются проблемы доверия, являющиеся фундаментальными среди проблем обеспечения безопасности облачных технологий. Для этого, в первую очередь, дается краткое объяснение понятия доверия, изученного в различных областях науки, исследуются технологии создания доверия на основе репутаций, подходы обеспечения прозрачности облачных технологий, методы установления доверия на основе соглашения об уровне сервиса, услуги «Доверие как сервис». Определяются существующие недостатки в исследованных проблемах, и приводится ряд рекомендаций для устранения данных недостатков.

Ключевые слова: *облачные технологии, доверие, соглашение об уровне услуг, репутация, Сибил атака*.

Rasim M. Alguliev[1], Fargana C. Abdullayeva[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]director@iit.ab.az, [2]farqana@iit.ab.az

An investigation of trust problems of the Cloud Computing

The paper investigates the trust problems which is a fundamental issue among security problems of cloud computing. For this purpose first of all the trust notion studied by various scientific fields is clarified. Technologies of developing of the reputation based trust, approaches to ensure transparency in the clouds, methods of establishing trust on the basis of service level agreements, mechanisms which provide trust as service are studied. As a result, existing problems in the trust mechanizms are identified, and number of recommendations for these problems solution is offered.

Keywords: *Cloud computing, trust, service level agreement, reputation based trust, Sybil attack.*