**UOT 004.7**

***Ələkbərov R.Q., Ələkbərov O.R.***
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rashid@iit.ab.az, oqtayalakbarov@yahoo.com

# MOBİL HESABLAMA BULUDLARINDA TƏHLÜKƏSİZLİK VƏ KONFİDENSİALLIQ MƏSƏLƏLƏRİ

*Məqalədə mobil hesablama buludlarında istifadə edilən bulud platformalarda təhlükəsizlik və məxfilik problemləri tədqiq edilmişdir. Mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkə təhlükəsizliyi istiqamətində meydana çıxan təhdidlər analiz olunmuşdur. Eyni zamanda məqalədə mobil hesablama buludlarında informasiya təhlükəsizliyi, konfidensiallıq, məlumatların yerləşdirilməsi və yerdəyişməsi, məlumatların tamlığı, kiber hücumlar və s. məsələlər də geniş təhlil olunmuşdur. Mobil hesablama buludlarının informasiya təhlükəsizliyi və konfidensiallığı məsələlərinin elmi-nəzəri problemləri araşdırılmış və bu istiqamətdə elmi- tədqiqat işlərinin vəziyyəti analiz edilmişdir.*

***Açar sözlər:*** *mobil hesablama buludları, mobil avadanlıqlar, informasiya təhlükəsizliyi, kiber hücumlar, hesablama və yaddaş resursları, hesablama buludları, virtual maşın, bulud xidmətləri.*

## Giriş

Hazırda dünyada hesablama buludları (*ing. Cloud Computing*) texnologiyasının köməyi ilə verilənlərin emalı mərkəzlərinin hesablama və yaddaş resurslarından səmərəli istifadə etmək istiqamətində intensiv tədqiqat işləri aparılır. Böyük hesablama və yaddaş resurslarına malik olan belə sistemlər yüksəksürətli əlaqə kanalına malik olan kompüter şəbəkələri əsasında yaradılır. Son dövrlərdə bulud texnologiyalarında yeni xidmətlərin meydana gəlməsi, mobil qurğular üçün mobil proqram əlavələrinin yaradılması qeyd edilən texnologiyalar əsasında mobil hesablama sistemlərinin yaradılmasına təkan vermişdir. Hazırda Cloud Computing texnologiyalarının xidmətlərindən mobil istifadəçilər də geniş istifadə edirlər. Dünyada mobil qurğuların (noutbuk, planşet, smartfonların və s.) istifadəsinin sürətlə artması və onların uyğun telekommunikasiya texnologiyalarının (GPS, 3G, 4G, Wi-Fi və s.) köməyi ilə İnternet üzərindən hesablama buludlarına qoşulması, yeni texnologiyanın – mobil hesablama buludları (*ing. Mobile Cloud Computing*) texnologiyasının yaradılmasına təkan verdi. Məlumdur ki, istənilən mobil qurğunun imkanları (hesablama və yaddaş resursları) məhdud səviyyədə olur. Amma istifadəçilər bu qurğuları böyük hesablama və yaddaş resursları tələb edən məsələlərin həllində istifadə edirlər. Bunun üçün hesablama buludları texnologiyalarından geniş istifadə olunur. Beləliklə, bulud texnologiyalarından istifadə etməklə mobil istifadəçilərin qurğularında olan hesablama və yaddaş resursları çatışmazlığını aradan qaldırmaq olar. Son dövrlərdə də bulud xidmətlərinin qiymətlərinin ucuzlaşması mobil istifadəçilərin həmin xidmətlərdən geniş istifadəsinə imkan yaradır.

İstifadəçilərin və müəssisələrin böyük həcmli məlumatlarının buludda yerləşdirilməsi və istifadə olunması onların hakerlər tərəfindən daha çox hücumlara məruz qalmasına səbəb olur və mobil istifadəçilərə gizliliklə bağlı problemlər yaradır [1, 2]. Bununla bağlı mobil qurğuların təhlükəsizliyinə təsir edən təhdidlər və mobil hesablama buludları sahəsindəki risklər araşdırılmış və tövsiyələr verilmişdir. Mobil hesablama mühitinin əsas məqsədi bulud xidməti provayderləri vasitəsi ilə İnternet üzərindən mobil istifadəçiləri proqram əlavələri və xidmətləri ilə təchiz etməkdir. Beləliklə, mobil hesablama buludlarında istifadəçilərin bulud serverlərdə yerləşmiş tətbiqi proqramlara əlyetərliyini təmin etmək üçün şəbəkənin müxtəlif hissələrində: mobil qurğularda, şəbəkədə, mobil proqram əlavələrində və təhlükəsizlikdə yaranan problemləri analiz etmək vacibdir.

Məqalədə mobil hesablama buludlarının istifadəsində meydana çıxan informasiya təhlükəsizliyi və fərdi məlumatların konfidesiallığı problemləri geniş şəkildə araşdırılmışdır.

**Mobil hesablama buludu platformalarında və mobil qurğularda təhlükəsizlik məsələləri**

Bulud texnologiyalarında proqram əlavələri və məlumatlar fərdi mobil qurğularda yox, əsasən İnternet şəbəkəsinin bulud serverlərində yerləşdirilir, saxlanılır və istifadəçilərin tələblərinə uyğun onlara təqdim olunur. Mobil hesablama buludlarında böyük hesablama və yaddaş resursları tələb edən verilənlər və proqram təminatı yerinə yetirildiyindən, mobil qurğuların güclü texniki imkanlara malik olmasına ehtiyac duyulmur.

Mobil hesablama buludları mobil qurğuların hesablama buludlarının xidmətlərindən istifadə edən yeni şəbəkə konsepsiyasıdır.

Hesablama buludlarında ənənəvi təhlükəsizlik məsələləri hələ də mövcuddur. Lakin müəssisənin imkanlarının və sərhədlərinin bulud xidmətlərindən istifadə edilməsi istiqamətində genişləndirilməsi səbəbindən ənənəvi təhlükəsizlik mexanizmləri buluddakı tətbiqi məlumatların məxfiliyini təmin edə bilmir. Buludların açıqlığı və çoxsaylı xidmətlərin xüsusiyyətləri mobil hesablama buludlarının informasiya təhlükəsizliyinə böyük təsir göstərir [3, 4] :

- Bulud platformalarında istifadə olunan proqram əlavələri və saxlanan məlumatlar sabit infrastruktura və təhlükəsizlik sərhədlərinə malik deyil. Bu, təhlükəsizliyin pozulması halında təhlükəyə məruz qalan fiziki resursları təcrid etməkdə çətinlik törədir;
- İstifadəçi və təşkilatlara bulud xidmətləri təklif edən bulud platformaları çoxsaylı provayderlərə məxsus və ya onların istifadəsində ola bilər. Bu isə maraqların müxtəlifliyini nəzərə alaraq, buludda mübahisəli bir hadisə baş verdikdə, onun həllinə vahid təhlükəsizlik tədbirləri tətbiq etməyi çətinləşdirir;
- Buludun açıqlığı və çoxsaylı istifadəçilərin buludun virtual resurslarından istifadəsi icazəsi olmayan şəxslərin istifadəçilərin məlumatlarına giriş əldə etməsinə imkan yaradır;
- Bulud platformaları çoxsaylı məlumatların saxlanmasını və bu məlumatlara sürətli çıxışı təmin etdiyi üçün, uyğun olaraq, bulud təhlükəsizlik tədbirləri də məlumatların emal ehtiyaclarını təmin etməlidir.

SPI (SaaS, PaaS, IaaS) xidmətlərinin təqdimat modelləri, yerləşdirmə modelləri və buludun əsas xüsusiyyətlərinin yaratdığı təhlükəsizlik problemləri infrastrukturun bütün aspektlərinə, o cümlədən, şəbəkə səviyyəsinə, host səviyyəsinə və tətbiq səviyyəsinə təsir edir. Qeyd edilən bulud platformalarında meydana çıxan təhlükəsizlik problemlərinə baxaq.

*IaaS platforması*nda *meydana çıxan problemlər*. Bulud texnologiyalarında istifadəçiləri hesablama resursları ilə təmin etmək üçün bulud serverlərdə yaradılan virtual maşınlardan (VM-dən) istifadə edirlər. Ona görə də VM-in təhlükəsizliyi əsas məsələlərdəndir. Məqsəd ümumi təhlükəsizlik həllərindən istifadə edərək VM-in əməliyyat sistemlərinin və proqram əlavələrinin fiziki serverlərə təsir edən zərərli proqram və viruslardan qorunmasıdır. VM-nin təhlükəsizliyi bulud istehlakçılarının məsuliyyətindədir. Hər bir bulud istehlakçısı (istifadəçi) özünün təhlükəsizliyinə nəzarət vasitələrindən istifadə edərək gözlənən riskin səviyyəsini müəyyən edib, onu aradan qaldıra bilməlidir [5, 6]:

- VM surətlərinin (*ing. image repository*) saxlanması. Fiziki serverlərdən fərqli olaraq, VM-lər avtonom rejimdə olduqda da, risk altında olurlar. VM surətləri VM-də yerləşən fayllara zərərli kodlarla təsir etməklə sıradan çıxarıla bilər və eyni zamanda onda olan məlumatların oğurlanması mümkündür. VM surətlərinin etibarlı qorunması bulud provayderləri tərəfindən həyata keçirilir. VM şablonları ilə bağlı başqa bir məsələ ondan ibarətdir ki, istifadəçinin ilkin məlumatları şablonlarda saxlanıla bilər və yeni istifadəçi bu surətləri istifadə etdikdə, gizlilik məsələlərini poza bilər;
- Virtual şəbəkə təhlükəsizliyi: eyni şəbəkə infrastrukturunda yerləşən serverlərdən müxtəlif kirayəçilərin (arendatorların) birgə istifadə etməsi fiziki serverlərə və DNS-serverlərə müdaxilə ehtimalını artırır;
- VM-in sərhədlərinin təhlükəsizliyi: VM fiziki serverlərlə müqayisədə virtual sərhədlərə malikdir. Bir fiziki serverdə yaradılan VM-lər eyni prosessordan, yaddaşdan, giriş-çıxış və şəbəkə

adapterindən istifadə edirlər (VM resursları arasında heç bir fiziki təcrid yoxdur). VM-ın sərhədlərinin təmin edilməsində bulud provayderləri məsuliyyət daşıyırlar.

*PaaS platformasında təhlükəsizlik məsələləri***:** proqram əlavələri interfeysinin təhlükəsizliyi. PaaS xidməti istifadəçilərə idarəetmə funksiyasını, təhlükəsizlik funksiyasını, proqram əlavələrin idarəsini həyata keçirən proqram əlavələri interfeysini (PƏİ) təklif edir. Təklif olunan PƏİ identifikasiya (həqiqilik) və avtorizasiyanı təmin edən təhlükəsizlik mexanizmləri ilə təchiz olunmalıdır [6].

*SaaS platformasında təhlükəsizlik məsələləri:* SaaS modelində təhlükəsizliyin təmin edilməsi bulud xidmətləri və proqram təminatları təklif edən təşkilatların birgə səyi nəticəsində həyata keçirilir. Bu model əvvəlki iki modeldə müzakirə edilən təhlükəsizlik məsələlərini özündə əks etdirməklə verilənlərin və şəbəkənin təhlükəsizliyinin idarə edilməsini özündə birləşdirir [7].

*Veb-əlavələrin dayanıqlığının yoxlanılması (skan edilməsi):* bulud infrastrukturunda yerləşdiriləcək veb-əlavələrin təhlükəsizliyi veb-əlavə skanerləri vasitəsi ilə yoxlanılmalıdır [8]. Veb əlavələr üçün yaradılan *firewallar* mövcud boşluqların tapılmasına imkan verilməlidirlər.

Qeyd edilən təhlükələrin məqsədi istifadəçilərin şəxsi məlumatlarının (məs: kredit kart nömrələri, parol, kimlərlə əlaqədar olması, yerləşmə yeri və s.) əldə edilməsi (oğurlanması) və ya onların mobil qurğularının resurslarından istifadə edilməsidir.

Mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkənin təhlükəsizliyi əsas məsələlərdəndir.

*Mobil istifadəçilərin təhlükəsizliyi.* Mobil qurğular müxtəlif təhlükəsizlik təhdidləri ilə (ziyanlı proqram kodları, virus proqramları və s.) üzləşirlər. Məsələn, GPS (*ing. Global Positioning System- Qlobal Yerləşmə Sistemi*) texnologiyalarının proqram əlavələrindən istifadə etdikdə məlumatların məxfiliyinin qorunması ilə bağlı problemlər yaranır. Ona görə də mobil qurğuların təhlükəsizliyi üçün təhdidləri müəyyən edən təhlükəsizlik proqram təminatları yüklənməsi tövsiyə olunur. Şəbəkədə istifadə edilən müxtəlif mobil qurğularda təhlükəsizliyi təhdid edən ziyanverici proqramlar mobil istifadəçilərdə məxfilik məsələlərində problemlər yaradır. Mobil istifadəçi təhlükəsizliyi ilə bağlı iki əsas məsələ var: mobil əlavələrin təhlükəsizliyi və məxfilik (konfidensiallıq). Təhlükəsizlik problemlərinin yoxlanılmasının ən əsas üsulu mobil qurğularda təhlükəsizlik proqramının və antivirusun quraşdırılması və işlənməsindən ibarətdir. Mobil qurğuların resursları məhdud olduğu üçün təhdidlərdən qorunmaq fərdi kompüterlərə nəzərən daha çətin olur. Təhlükənin aşkarlanması və təhlükəsizlik mexanizmlərinin buluda ötürülməsi üçün bir neçə üsul tətbiq edilir. Mobil istifadəçilər proqram əlavələrindən istifadə etməzdən əvvəl, bir sıra təhlükələrin qiymətləndirilməsi prosedurlarından keçməlidirlər. Mobil qurğularda proqram əlavələri ilə yerinə yetirilən bütün hərəkətlər zərərli olub-olmamasına aid yoxlamadan keçirilməlidir. Bütün bunlarla yanaşı, mobil qurğular antivirus proqramların bulud təhlükəsizlik serverlərində də yerinə yetirilməsi prosesinə nəzarət edirlər [9]. Mobil hesalama buludlarında verilənlərin təhlükəsizlik və gizlilik problemlərinə nəzər yetirək. Mobil qurğuların əksəriyyəti qorunmadığından və ya zəif qorunduğundan onlardan məlumatların itməsi və oğurlanması ehtimalı daha böyükdür. Məlumatlara icazəsi olmayan şəxs mobil qurğulara çox asanlıqla daxil olub, məlumatları asanlıqla əldə edə bilər.

*Mobil qurğuların təhlükəsizliyinə təsir edən təhdidlər* [4–10]:

- İtirilmiş və ya oğurlanmış mobil qurğularda məlumat itkisi;
- Mobil zərərli proqram təminatları vasitəsi ilə məlumatların oğurlanması;
- Proqram əlavələrin boşluğundan istifadə edərək məlumatların sızması;
- Qurğuların və əməliyyat sistemlərinin daxilindəki boşluqlar;
- Təhlükəsiz şəbəkəyə giriş və etibarsız giriş nöqtələrinin olması;
- Təhlükəli bulud proqram əlavələrinin olması;
- Proqram əlavələri interfeyslərinin etibarlı idarəetmə imkanlarının olmaması.

Simsiz rabitə zamanı məlumatlar bədniyyətlilər (hakerlər) tərəfindən hücumlara məruz qala bilər. Birdən çox giriş nöqtəsindən məlumatlara daxil olmaq əlaqə kanalında yüklənməyə səbəb ola

bilər. Bu isə məlumatlardan müəyyən xidmətlərin istifadəsini bloklaya (kilidləyə) bilər. Mobil cihazlarda məlumatların itməsinin qarşısını almaq üçün zərərli proqramlar izlənməli və onları zərərsizləşdirmək üçün antivirus proqramlardan istifadə olunmalıdır. Bu proqramlar zərərli proqramlara nəzarət edir. Zərərli kod (proqramlar) yalnız virus proqramları deyil. Zərərli proqramlar ziyanverici sosial şəbəkələrdə meydana çıxan fişinq proqramları, spamları, şəxsi məlumatların oğurlanmasını həyata keçirən zərərli proqramları özündə birləşdirir. Bədniyyətlilərin şəbəkəyə daxil olmasının qarşısını almaq üçün simsiz protokol şifrələməsindən istifadə etməklə təhlükəsiz rabitə kanalı yaradılır. Mobil qurğu və bulud arasında məlumatların mübadiləsində təhlükəsizlik və gizlilik həmişə əsas məsələ olmuşdur.

Mobil hesablama buludlarının serverlərində məlumatların təhlükəsizliyinin təmin olunması məsələsinə baxaq. Bulud serverlərində istifadəçi verilənlər üzərində nəzarəti həyata keçirə bilmir və məlumatların buludlarda hansı serverlərdə yerləşdirilməsi haqqında məlumatı da olmur. Belə hallarda məlumatların fiziki daşıyıcılarının sıradan çıxması və ya məlumatların müəyyən şəxslər tərəfindən qərəzli silinməsi nəticəsində də itməsi mümkündür.

**Mobil hesablama buludlarında təhlükəsizlik və məxfilik məsələləri**

Mobil buludlarda məlumatların təhlükəsizliyi məsələlərinə nəzər yetirək. Müştəri məlumatlarını buludda yerləşdirərkən ona həmin məlumatlara girişin yalnız səlahiyyətli səxslərin girişi ilə məhdudlaşdırılacağına zəmanət verilməlidir. Bulud provayderlərinin heyəti tərəfindən müştərinin şəxsi məlumatlarına qeyri-qanuni giriş bulud məlumatları üçün potensial təhlükələrdən biri hesab olunur. Bundan əlavə, provayderlər tərəfindən bulud istifadəçilərinin məlumatlarının təhlükəsizliyini təmin etmək üçün müştərilərə təlimlər keçirilməli, onlar konfidensiallıq siyasəti və prosedurlarla təmin edilməlidirlər. Bulud istifadəçisi buludda saxlanılan bütün məlumatların təhlükəsizliyinin qorunmasına əmin olmalıdır.

Mobil hesablama buludlarında təhlükəsizlik məsələləri aşağıdakılardır:

- *İnformasiya təhlükəsizliyi.* Mobil buludlar əsasən məlumatların (verilənlərin) saxlanması və emalı ilə əlaqədar olduğundan, burada təhlükəsizlik çox böyük əhəmiyyətə malikdir. Hazırda müxtəlif bulud platformaları daxildə quraşdırılmış təhlükəsizlik tədbirləri təklif edirlər. SSL (*ing. Secure Sockets Layer*) kriptoqrafik protokol olub, mobil istifadəçi ilə bulud server arasında əlaqə kanalında təhlükəsizliyi təmin edir [11]. Məlumatların təhlükəsizliyi məsələsinə gəldikdə, şirkətlər məlumatların və əməliyyatların təhlükəsizlik siyasəti və prosedurlarını həyata keçirməlidirlər. Provayderlər siyasət və prosedurların tam yerinə yetirildiyinə əmin olmaq məqsədilə OPSEC (*ing. Open Platform for Secure Enterprise Connectivity – şəbəkəyə təhlükəsiz qoşulmaq üçün açıq platforma*) haqqında istifadəcilərə ümumi şəkildə şirkət təlimləri, tədris və təlimatlar da keçirə bilərlər. Girişə nəzarət, autentifikasiya prosedurları, istifadəçi idarəetməsi, şifrələmə, kontent təchizatı və ümumi kommunikasiya təhlükəsizliyi ilə əlaqədar siyasətlər hazırlanmalı və onların qüvvədə olması üçün müəyyən tədbirlər görülməlidir [12]. İstifadəçi məlumatlarının və tətbiqlərin təhlükəsizliyinin və məxfiliyinin təmin olunması haqqında provayder tərəfindən istifadəçiyə zəmanətin verilməsi çox vacibdir. Bu, bulud xidməti təklif edən istehsalçının mobil platformasına inamın yaranmasına imkan verir. İtirilmiş və ya oğurlanmış qurğuların məsafədən təmizlənməsi ilə mobil qurğudakı məlumatların sui-istifadəsinin qarşısını almaq mümkündür. Bu xüsusiyyət, ümumiyyətlə, əksər mobil istehsalçı və mobil istifadəcilər tərəfindən təmin olunur [13]. Mobil qurğular (mobil telefon, PDA, smartfon və s.) zərərli kodlar (məs., virus, soxulcan və troyan atı və s.) kimi bir sıra təhlükələrə qarşı çox həssasdırlar. Mobil qurğuların Qlobal Yerləşmə Sistemində (*ing. GPS-Global Positioning System*) işləməsi təhlükəsizlik məsələlərində problemlərin yaranmasına səbəb ola bilər. İstənilən mobil qurğunun təhlükəsizlik problemlərinin aşkarlanmasının ən sadə yolu onlarda təhlükəsizlik proqram təminatının (Kaspersky, McAfee və AVG antivirus proqramları) quraşdırılması və istifadəsidir. Buna baxmayaraq, mobil qurğuların məhdud emal gücü və enerji təchizatı olduğuna görə, onların təhlükələrdən qorunması digər kompüter qurğularına (məs., fərdi kompüter) nisbətən daha çətindir. Bunun üçün isə təhlükələrin

aşkarlanma imkanlarını buluda köçürmək mümkündür. Bu paradiqma təhlükənin buludda quraşdırılmış aşkarlama xidmətini təmin edən mövcud Cloud AV platformasının quraşdırılması və istifadəsidir. Bu, həmçinin paralel olaraq bir neçə antivirus sistemlərini virtuallaşdırılmış konteynerlərdə saxlamaqla istifadə edilməsinə imkan verir. Bu yanaşma, təhlükələrin səmərəli aşkarlanmasına imkan verir və enerji sərfiyyatını 30%-dək azaldır. Böyük həcmdə məlumat və tətbiqlərin buludda saxlanmasının bir sıra üstünlüklərə malik olmasına baxmayaraq, məlumat və tətbiqlərin tamlığı, autentifikasiya və istifadəçi hüquqlarının qorunması məsələləri də nəzərə alınmalıdır [14].

• *Konfidensiallıq və gizlilik.* Mobil istifadəçinin coğrafi yerinin aşkarlanması istifadəçinin vacib məlumatlarının (doğum tarixi, kredit kart məlumatları, şəxsi məlumatlar, xəstəlik tarixçəsi və s.) konfidensiallıq və gizlilik məsələlərinə dair problemlər yaradır [15]. Mobil qurğular GPS texnologiyasından istifadə edirlərsə, bu onların fiziki yerini təyin etməyi çox asanlaşdırır. Müəssisələrin məlumatlarının təhlükəsizliyini yalnız müəyyən bulud xidmətlərinin analiz və təhlil edilməsi vasitəsi ilə yüksəltmək olar. İstifadəçinin məlumatları bulud serverlərdə yerləşdirildikdən sonra, həmin məlumatlara girişin yalnız səlahiyyətli icazəsi olan şəxslər ilə məhdudlaşacağına dair bir zəmanət olmalıdır. Bulud personalı tərəfindən icazəsiz istifadəçi məlumatlarına daxilolma şəxslərin bulud məlumatlarına potensial təhlükə yarada biləcək bir riskdir. Müştərilərə təminatlar verilməli və müvafiq qaydalar tətbiq edilməli, konfidensiallıq siyasəti və prosedurları istifadəçilərin məlumatlarının bulud serverlərdə təhlükəsizliyini təmin etməlidir. Konfidensiallığın pozulması riski, oğurluq halları və fırıldaqçılıq məlumatların bir-biri ilə qarşılıqlı əlaqədə olan sistemlər arasında paylanması üçün bir sıra tədbirlərin görülməsi, monitorinqin aparılması, protokolların qəbul olunması və istifadəçiləri sosial media təhlükəsizliyi haqqında məlumatlandırmaqla azaldıla bilər. Sosial mediadan istifadə haqqında siyasətin hazırlanması və infrastrukturun qorunması üçün bir neçə prosedurun aparılması ilə şirkətlər özlərinin hüquqi və təhlükəsizlik problemlərini həll edə bilərlər. Əks təqdirdə, onların informasiya infrastrukturu və reputasiyası ziyan görə bilər [16]. Məlumatların tamlığını və konfidensiallığnı qorumağın ən effektiv yolu şifrləmədir. Şifrləmə məlumatların saxlanması və ötürülməsinə imkan verməklə əsasən onun emalını kənar müdaxilələrdən qoruyur [17]. GPS qurğuları mobil istifadəçilərə lokal əsaslı xidmətlərdən (LƏX) istifadə etmək imkanı verir. Lakin mobil istifadəçi bu sistemdən istifadə edərək özünün şəxsi məlumatını paylaşdıqda, LƏX gizliliklə bağlı problemin yaranmasına səbəb ola bilər. Bu problemi aradan qaldırmaq üçün Lokasiya etibarlı serverlərdən (LES) istifadə edirlər [18]. Rəqəmsal hüquq idarəetməsi (RHİ) isə digər məxfilik probleminin həllini təmin edir. Strukturlaşdırılmamış rəqəmsal kontent (məs., video, foto, audio, e-kitab və s.) adətən piratçılıq və qeyri-qanuni yolla paylaşılır. Onların piratçılıq və qeyri-qanuni yolla paylanmasının qarşısını almaq məqsədilə SİM kartlı bulud-əsaslı rəqəmsal mobil hüquq idarəetməsi sxemi olan Phosphor təklif edilmişdir [19]. O, çevikliyi artırır və çox aşağı qiymətə təhlükəsizlik boşluqlarını aradan qaldırır. Lakin bu yanaşma əsasən mobil telefonların SİM kartına əsaslandığına görə, o, Wi-Fi vasitəsilə həmin kontentlərə daxil olan noutbuk kimi qurğulara tətbiq edilə bilmir [20].

• *Məlumatların tamlığı.* Məlumatların təhlükəsizliyini təmin etməklə bulud xidmət provayderləri məlumatların tamlığını qorumaq və müəyyən məlumat toplularının (dəstlərinin) harada və hansı vəziyyətdə olduğunu təsvir etmək üçün müəyyən mexanizmlər həyata keçirməlidirlər. Bulud provayderi buludda xüsusi verilənlərin yerləşdirildiyi, onların mənşəyi və tamlıq mexanizmləri haqqında müştəriyə xəbərdarlıq etməlidirlər.

• *Məlumatların yerləşdirilməsi və yerdəyişməsi.* Bulud verilənlərin yüksək mobilliyini təklif edir. İstehlakçılar öz məlumatlarının yerləşdiyi yeri hər zaman bilmirlər. Buna baxmayaraq, istifadəçi buluddakı saxlama qurğusunda hər hansı konfidensial məlumat saxladıqda, onun yerləşdiyi yerin göstərilməsini tələb edə bilər. Onlar, həmçinin üstünlük verdikləri yeri də göstərə bilərlər (məsələn, Hindistanda saxlanılan məlumatlar). Bu zaman bulud provayderi ilə istehlakçı arasında müqavilənin bağlanması tələb olunur. Həmin müqaviləyə əsasən, məlumatlar müəyyən bir serverdə və xüsusi yerdə saxlanmalıdır. Bundan əlavə, bulud provayderləri həmin sistemlərin

(məlumatlar da daxil olmaqla) təhlükəsizliyinin təmin edilməsinə və müştərilərin məlumatlarının qorunmasına görə məsuliyyət daşıyırlar. Digər məsələ isə məlumatların bir yerdən digərinə köçürülməsidir. Məlumatlar ilkin olaraq, bulud provayderləri tərəfindən müəyyənləşdirilmiş müvafiq yerdə saxlanılır. Buna baxmayaraq, bu məlumatlar təhlükəsizlik baxımından bir yerdən başqa yerə köçürülə bilər. Bulud provayderləri öz aralarında müqavilələr bağlayaraq bir-birinin resurslarından istifadə edə bilirlər.

• *Kiber hücumlar.* Bütün şəbəkələr bir və ya bir neçə zərərli hücuma (haker hücumuna) məruz qalırlar. Bütün Web 2.0 serverlərinin təhlükəsizliyinə nəzarət etməklə verilənlərə olan təhlükələri azaltmaq olar. Bundan əlavə, Web 2.0 serverləri digər daxili serverlərdən ayırmaqla gələcəkdə sosial media və veb saytlar vasitəsilə məlumatlara icazəsiz giriş təhlükəsini aradan qaldırmaq mümkündür [21]. Potensial hücumlara aşağıdakılar aid ola bilər:

✓ *Xidmətdən imtina (ing. DoS- Denial of Service) hücumları.* Bulud serverləri daha çox DoS hücumlarına məruz qalır, çünki eyni zamanda birdən çox müştəri buluda müraciət edə bilər, bu isə DoS hücumlarını daha effektli edə bilər;

✓ *Kanala* kənar hücumlar. Bu növ hücumlarda hakerlər zərərli VM yaratmaqla, onu hər dəfə alınmış bulud serverinə yaxın məsafədə yerləşdirirlər və müəyyən müddətdən sonra bulud serverin təhlükəsizliyi risk altına alınır və daha sonra məlumat ötürmə kanalına kənardan hücum edilir;

✓ *Autentifikasiya hücumları.* Virtual xidmətlər sahəsində autentifikasiya problemi ən zəif nöqtələrdən biri hesab olunur. İstifadəçi hücumçular tərəfindən ən çox hədəfə alınmış identifikasiya proseslərini qorumaq məqsədilə bir sıra mexanizm və metodlardan istifadə edə bilər;

✓ *Vasitəçi insan ilə şifrləmə hücumları.* Bu hücum zamanı adətən hücumçu (haker) özünü iki istifadəçi arasına salır. Bu növ hücumlarda hücumçu kommunikasiya yolunda yerləşir, daha sonra isə hər şey onun özündən asılı olur. Belə ki, o, rabitəyə müdaxilə edə və ya onun istiqamətini dəyişdirə bilər [22].

*Şəbəkə monitorinqi.* Gecikmə və əhatə problemlərindən əlavə, şəbəkənin fəaliyyətinin monitorinqi də həlli vacib məsələlərdən biridir. Trafikin yenidən yönləndirilməsi, giriş mübadiləsi və xidmətin göstərilməsinə imkan verən dinamik bulud monitorinq sisteminin olması çox vacibdir. Digər tərəfdən, mobil hesablama buludlarında nasazlıqların, şəbəkədə baş verən gecikmələrin operativ müəyyən edilməsi və təhlükəsizlik məsələlərinin həll edilməsi üçün monitorinqin aparılmasına ehtiyac yaranır. Müvafiq şəbəkə monitorinqi olmadan hər hansı şirkət dəyərli informasiyaların yayılması ilə əlaqədar siyasətə istifadəçilərin nə dərəcədə əməl etdiyini müəyyənləşdirə bilməz. Bundan əlavə, Web 2.0 tətbiqlərində (məs., Java, AJAX və JSON verilənlərin mübadilə formatı) istifadə edilən proqramlaşdırma dilləri də zərərli proqramların şirkətin şəbəkə infrastrukturuna daxil olmasına və ona ziyan vurmasına (məs., məlumat və ya tətbiqlərə giriş əldə etmək və ya onları məhv etmək) imkan yaradır. Buna görə də, sosial mediadan istifadə edən hər bir şirkət şəbəkə infrastrukturunda yerləşən hər hansı informasiyanın qorunması üçün yüksək təhlükəsizlik nəzarətini yerinə yetirməlidir [23].

• *Uyğunluq və icra.* Hazırda mobil hesablama buludları üçün heç bir formal standart siyasət toplusu mövcud deyil. Lakin PCİDSS (*ing. Payment Card Industry Data Security Standard - Ödəniş Kartları Sənayesinin Verilənlərin Təhlükəsizlik Standartları)*, HIPAA (*ing. Health Insurance Portability and Accountability Act – Sağlamlıq Sığortasının Daşınma və Hesaba alınması Aktı*) standartlarında da verilənlərin saxlanması və istifadəsi üzrə bir sıra qaydalar mövcuddur [24]. Bu standartlar üçün mütəmadi hesabat və auditin keçirilməsi tələb olunur. Korporativ verilənlərin buluda köçürülməsi üçün bu qaydaların tam və müvafiq şəkildə yerinə yetirilməsi çox vacibdir. Verilənlər müəyyən hüquqi məhdudiyyətlərə malik olduqda və ya hər hansı qaydaya uyğun gəlmədikdə, açıq buludlardan istifadə çətinləşər və ya hətta qeyri-mümkün ola bilər. Bunun üçün provayderlər idarə olunan bazarların tələbatlarını ödəmək məqsədilə bulud infrastrukturlarını qurmalı və onların təhlükəsizlik standartlarına uyğunluğunu təsdiqlətməlidirlər.

Bulud haqqında ümumi anlayışlar da daxil olmaqla, bir sıra qeyri-texniki amillər səbəbindən sertifikatlaşdırma prosesi mürəkkəbləşə bilər. Belə ki, çoxsaylı təhlükəsizlik təhdidləri mövcuddur, onların hər birinin qarşısını almaq üçün tədbirlər görmək qeyri-mümkündür. İstifadəçi hər hansı tətbiqi icra etdikdə, o, istifadə ilə əlaqəli olan potensial təhlükəsizlik təhdidlərinin təbiəti və nəticələri barəsində anlayışa malik olmur. Bunun üçün istifadəçi şəbəkə və məlumatların təhlükəsizliyi üzrə təlimatlandırılmalıdır. Sosial mediaya gəldikdə isə, onların səbəb olduğu əlavə risklərin də aradan qaldırılması üçün təlim proqramları keçirilməlidir. Bu sosial media təlimləri təşkilatların illik təhlükəsizlik proqramlarına da şamil edilə bilər. Sosial media vasitələri və saytları da həmin sertifikatlaşdırma və akkreditasiya prosedurları zamanı həll edilə bilər və bununla da təşkilatın təhlükəsizlik standartları təmin oluna bilər. Bundan əlavə, təşkilat tərəfindən monitorinq proqramı da təşkil edilə bilər, bu zaman sosial media bacarıqları, texnologiyaları haqqında daha çox məlumatı olan işçilərin biliklərindən yararlanmaq olar [24].

• *İnsidentlərin cavablandırılması.* Verilənlər və məlumatların təhlükəsizliyini təmin etmək məqsədilə görülən tədbirlərdən və istifadəçilərin ən təhlükəsiz metodlar haqqında təlimatlandırılmasından sonra belə, insidentlər baş verə bilər. Hər bir bulud provayder təşkilatı verilənlərin itməsi və sui-istifadəsinin qarşısını almaq və zərərli hücumdan qorunmaq məqsədi ilə bəzi tədbirləri cəld şəkildə yerinə yetirmək üçün plan hazırlamalıdır. Əksər provayderlər onlara hücum edilə bilmədiyini iddia edərək, öz təhlükəsizlik xidmətlərini təkmilləşdirmirlər. Lakin qeyd etmək lazımdır ki, bulud-əsaslı xidmətlər hakerlərin diqqətini daha çox cəlb edir. Buna görə də, bu cür hücumlar baş verməzdən əvvəl tədbirlərin görülməsi daha məqsəduyğun hesab olunur. Başqa sözlə desək, hər hansı hücumun qarşısının alınması onun sonradan bərpa edilməsindən daha asandır [25].

Bir çox hallarda bulud istifadəçisi bulud xidmətlərinin fiziki baxımdan harada yerləşdiyi haqqında heç bir məlumata malik olmur. Lakin onlar da yanğın, qasırğa, təbii fəlakət və s. kimi təhlükələrlə üzləşirlər. Beləliklə də, bu baxımdan da onlar bir sıra tədbirlər görməlidirlər ki, əks təqdirdə, bulud provayderi həmin təhdidlərə cavab verə bilməz və davamlı xidməti təmin edə bilməz [26].

**Təhlükəsizlik və məxfilik məsələləri üzrə tədqiqat işləri**

Mobil hesablama buludlarının təhlükəsizlik və gizlilik məsələləri bir çox tədqiqatçılar tərəfindən tədqiq edilmişdir. Son dövrlərdə mobil hesablama buludlarında təhlükəsizlik və gizlilik məsələlərini daha etibarlı həll etmək üçün çoxbuludlu (*ing. multi-cloud*) sistemlərdən istifadə edirlər. Bu sistem imkan verir ki, istifadəçilər bir-birindən asılı olmayan provayderlərin xidmətindən istifadə etsinlər və bu da istifadəçilərin bir bulud provayderindən asılılığını aradan qaldırır. Eyni zamanda, bu sistem bir buludda problem yaranarsa, ondakı məlumatların digər buludlara köçürülməsi məsələsini aradan qaldırır. Bulud xidmətlərinin istifadəçiləri arasında bir qorxu var ki, bir buludlu sistem gizliliyi və təhlükəsizliyi təmin edə bilməz. Ona görə də onlar məlumatların saxlanması və emalı üçün çoxbuludlu sistemlərdən istifadə edirlər. Çoxbuludlu sistemlərin təhlükəsizlik məsələlərinin yüksək səviyyədə həll olunması haqqında çoxsaylı məqalələr çap olunur [27].

Təşkilat əməkdaşlarının lazımi məlumatlarını (kredit kartları və tibbi sağlamlığı haqqında məlumatlar və s.) çoxbuludlu sistemlərdə saxlamaqla, məlumatların istifadəyə icazəsi olmayan şəxslərdən və hakerlərdən qorunmasını təmin etmək olar [28].

Birbuludlu sistemdən çoxbuludlu sistemə keçdikdə, gizlilik və təhlükəsizlik məsələləri bir neçə provayder arasında paylanır və bu da istifadəçilər arasında sistemin etibarlılığına inamı artırır. İstifadəçilərin hər hansı buludda yerləşən məlumatlarından istifadəsində problemlər yaranarsa, bu məlumatların başqa buludlara yerdəyişməsinə ehtiyac qalmır, çünki o əvvəlcədən həmin məlumatları digər buludlarda yerləşdirdiyindən, bu tip problemlərdən asanlıqla yayınır [29].

İstifadəçilərin şifrlənmiş məlumatlarını müəyyən hissələrə bölərək, onları müxtəlif bulud serverlərində saxlamaqla təhlükəsizliyi və gizliliyi artırmaq olar [30].

Popovic və başqaları [31] öz tədqiqat işlərində bulud xidmətləri təklif edən provayderlərin üzləşdikləri təhlükəsizlik və gizlilik məsələlərini qeyd edirlər. Bulud serverlər uzaq məsafədə yerləşirlər və istifadəçilər VM vasitəsilə resurslara daxil olurlar. Bir fiziki maşında çoxsaylı VM yaradılır. Hər bir istifadəçi fərdi virtual mühitdə işləməsinə baxmayaraq, istifadə edilən VM-lər bir-birlərinə təhlükəsizliklə bağlı təhdidlər yaradır. Müəlliflər qeyd edilən təhdidləri aradan qaldırmaq üçün metod təklif edirlər.

Məlumatların təhlükəsizliyi məqsədi ilə mobil əlavələrin müxtəlif bulud xidmətləri ilə inteqrasiyasını təmin edən mobil hesablama buludlarının yeni arxitekturası təklif olunmuşdur [32]. Təklif olunan model mobil qurğularda məlumatların təhlükəsiz saxlanmasını və emalını yaxşılaşdırır. Model məlumatların tamlığının və təhlükəsizliyinin qorunmasına kömək edir .

G.Portokalidis və başqaları isə öz işlərində [33] Oberheide və digərləri tərəfindən aparılan CloudAV tədqiqatına əsaslanaraq, mobil qurğularda (smartfonlarda) yaranmış təhdidin aşkarlanması üçün sxem təklif etmişlər. Buludda müxtəlif növ hücumları paralel olaraq aşkar edən bir çox smartfon nüsxələri mövcuddur. Təklif olunan sxem isə ötürmə yükünü aşağı salır və enerji istehlakını 30% azaldır. Bu metodda bulud tam etibarlı hesab edilir.

İstifadəçilərin identifikasiyası mobil hesablama buludları mühitində problemli bir məsələdir. Kriptoqrafiya metodlarından məlumatların şifrələməsində və autentifikasiyada istifadə edildikdə, açarlar təhlükəyə məruz qaldıqda və ya itirildikdə resurslara çıxış əldə etmək çətinləşir. Buna görə mobil hesablama sistemlərində effektiv idarəetməyə ehtiyac yaranır. [34]-də profilləşdirmədən istifadə edərək identifikasiya modeli təklif edilir. Bu, istifadəçi və xidmət məlumatlarını özündə birləşdirilməsini təmin edir. Bununla belə, kompleks təhlükəsizlik alqoritmlərinin tətbiqi smartfonların məhdud resurslarını nəzərə alaraq yerinə yetirilməlidir [34].

*Phosphor* modeli təklif edilir. Burada SİM kart və Rəqəmsal Hüquqları İdarəetmə Agenti (*ing.Digital Rights Management Agent*) arasında qarşılıqlı əlaqə Lisenziya Statusu (*ing. License Status*) protokolu ilə dəstəklənir.

[35]-də təhlükəsiz məlumat xidməti üçün proksi yenidən-şifrləmə sxemi və identifikator-əsaslı şifrləmə sxeminə malik yeni model təqdim edilir. Bu sxemdə istifadəçi gizliliyi təmin edilir, belə ki, verilənlərin kriptoqrafik çevrilməsi istifadəçi tərəfindən aparılır, lakin bu, mobil qurğunun enerji və emal tələbatını artırır.

[36]-da zərərli proqramların mobil mühitdə yaradığı təhlükəsizlik məsələləri tədqiq edilmişdir. Bu zərərli proqramlar bir VM-ə təsir edərək, tez bir zamanda digərlərinə yayılırlar. Hücuma məruz qalan VM bulud istifadəçiləri üçün ciddi bir problem olan məlumatların sızmasına və itirilməsinə səbəb olur.

Müəlliflər Cloud AV platforması və zərərli proqramların aşkarlama sistemini təklif etmişlər. Bu modeldə istifadə edilən mobil agent ilk növbədə zərərli faylları təhlil edir. Onun siqnaturası keşlənmiş verilənlər bazası ilə uyğun gəlmədikdə, o, virtualizasiya metodunun köməyi ilə host maşınlarda paralel olaraq işə salınan çoxsaylı mexanizmlərin vasitəsilə zərərli faylları müəyyən etmək üçün şəbəkə servisinə göndərilir. Bu metodlar zərərli proqramları daha yaxşı aşkarlaya bilir. Qurğu proqram təminatının minimum mürəkkəbliyi və aşağı enerji istehlakı kimi üstünlüklərə, lakin kəsilən əməliyyat və təsadüfi gizlilik təhlükəsi kimi məhdudiyyətlərə mailkdir [37] .

**Nəticə**

Məqalədə mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və mobil hesablama buludları şəbəkəsinin təhlükəsizliyi məsələləri təhlil olunmuşdur. Mobil hesablama buludlarının istifadəsi zamanı meydana çıxan təhlükəsizlik və gizlilik problemləri araşdırılmış və həlli yolları göstərilmişdir. Məqalədə mobil hesablama buludlarında informasiya təhlükəsizliyi, konfidensiallıq, məlumatların yerləşdirilməsi və yerdəyişməsi, məlumatların tamlığı, kiber hücumlar və s. məsələlər geniş təhlil olunmuşdur. Mobil hesablama buludlarının təhlükəsizlik və məxfilik məsələlərində meydana çıxan problemlər araşdırılmış və bu istiqamətdə elmi-tədqiqat işlərinin vəziyyəti analiz edilmişdir.

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

**Ədəbiyyat**

1. Gayathri M.R., Srinivas K. A Survey on Mobile Cloud Computing Architecture, Applications and Challenges // International Journal of Scientific Research Engineering & Technology, 2014, vol.3, no.6, pp.1013–1021.
2. Qi H., Gani A. Research on mobile Cloud Computing: review, trend and perspectives / Proceeding of IEEE second international Conference on Digital Information Technology & its application, 2012, pp.195–201.
3. Xiao Z., Xiao Y. Security and Privacy in Cloud Computing // IEEE Communications Surveys & Tutorials, 2013, vol.15, no.2, pp.843–859.
4. Gopichand M. An Overview of Security and Privacy Issue in Mobil Cloud Computing Environment // International Jornal of Advanced Researc in Computer Science and Software Engineering, 2016, vol.6, no.5, pp.779–784.
5. Hlavacs H., Treutner T., Gelas J.P., Lefevre L. Orgerie A.C. Energy consumption side-channel attack at virtual machines in a cloud / IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), 2011, pp.605–612.
6. Caytiles R., Lee S. Security considerations for Public Mobile Cloud Computing // International Journal of Advanced Science and Technology, 2012, vol.44, pp.81–88.
7. Chen Y., Paxson V., Katz R.H. What's New About Cloud Computing Security? Electrical Engineering and Computer Sciences University of California at Berkeley.Technical Report, no. UCB/EECS-2010-5, 2010, pp.1–8.
8. Chen Y.J., Wang L.C. A security framework of group location-based mobile applications in cloud computing / Proceeding International Conference on Parallel Processing Workshops, (ICPPW'11), 2011, pp.184–190.
9. Subashini S., Kavitha V. A survey on security issues in service deliverymodels of cloud computing // Journal of Network and Computer Applications, 2011, vol.34, pp.1–11.
10. Fernando N., Seng L.W., Rahayu L. Mobile Cloud Computing: A Survey // Journal of Future Generation Systems, 2013, vol.29, no.1, pp.84–106.
11. Donald A., Oli S., Arockiam L. Mobile cloud security issues and challenges: A perspective // International Journal of Engineering and Innovative Technology, 2013, vol.3, no.1, pp.401.
12. Sarrab M. Mobile Cloud Computing: Security Issues and Considerations // Journal of Advances in Information Technology, 2015, vol.6, no.4, pp.248–251.
13. Collings R. Mobile Cloud Adoption Challenges in the Enterprise. http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-theenterprise/
14. Dinh H.T., Lee C., Niyato D., Wang P. A survey of mobile cloud computing: Architecture, applications, and approaches // Wireless Communications and Mobile Computing, 2013, vol.13, no.18, pp.1587–1611.
15. Bahar A., Habib A., Islam M. Security architecture for mobile cloud computing // International Journal of Scientific Knowledge Computing and Information Technology, 2013, vol.3, no.3, pp.11–17.
16. Jashizume K. H., Rosado D., Fernandez-Medina E., Eduardo B. An analysis of security issues for cloud computing // Journal of Internet Services and Applications, 2013, vol.4, no.5, pp.1–13.
17. Schoo P., Fusenig V., Souza V., Melo M., Murray P., Debar H., Medhioub H., Zeghlach D. Challenges for Cloud Networking Security / 2nd International ICST Conference on Mobile Networks and Management, 2010, pp.2–16.
18. Zhangwei H., Mingjun X. A Distributed Spatial Cloaking Protocol for Location Privacy / Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010, vol.2, pp.468–471.

19. Zou P., Wang C., Liu Z., Bao D. Phosphor: Cloud Based DRM Scheme with Sim Card / Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), 2010, pp.459–463.
20. Zhu Y., Hu H., Ahn G.J., Huang D., Wang S. Towards temporal access control in cloud computing / INFOCOM, 2012, pp.2576–2580.
21. Lakshmi I. A Review on Cloud Computing in Mobile Applications. // International Journal of Computer Science and Mobile Computing, 2016, vol.5, no.6, pp.149–161.
22. Gregg M. 10 Security Concerns for Cloud Computing. Global Knowledge, 2010, pp.2–7.
23. Sarrab M., Janicke H. Runtime monitoring and controlling of information flow // International Journal of Computer Science and Information Security, 2010, vol.8, no.9, pp.37–45.
24. Chow R., Jakobsson M., Masuoka R., Molina J., Niu Y., Shi E., Song Z. Authentication in the clouds: a framework and its application to mobile users / Proceeding ACM Cloud Computing Security Workshop (CCSW'10), 2010, pp.1–6.
25. Huang D., Zhou Z., Xu L., Xing T., Zhong Y. Secure data processing framework for mobilecloud computing / Proceeding IEEE INFOCOM Workshop on Cloud Computing, (INFOCOM'11), 2011, pp.620–624.
26. Yogita D.M., Kailas K.D. Protection concern in Mobile Cloud Computing - A Survey // IOSR Journal of Computer Engineering (IOSR-JCE), pp.39–44.
27. AlZain M., Pardede E., Soh B., Thom J. Cloud computing security: From single to multi-clouds/45th Hawaii International Conference on System Science (HICSS), 2012, pp.5490–5499.
28. Cachin C., Keidar I., Shraer A. Trusting the cloud // ACM SIGACT News, 2009, vol.40, no.2, pp.81–86.
29. Vukolic M. The byzantine empire in the intercloud // ACM SIGACT News, 2010, vol.41, no.3, pp.105–111.
30. Shankarwar M., Pawar A. Security and privacy in cloud computing: A survey / Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, ser. Advances in Intelligent Systems and Computing. Springer International Publishing, 2015, vol.328, pp.1–11.
31. Popovic K., Hocenski V. Cloud computing security issues and challenges / MIPRO, Proceedings of the 33rd International Convention, 2010, pp.344–349.
32. Kovachev D., Klamma R. Framework for Computation Offloading in Mobile Cloud Computing // International Journal of Artificial Intelligence and Interactive Multimedia, 2012, vol.1, no.7, pp.6–15.
33. Portokalidis G., Homburg P., Anagnostakis K., Bos H. Paranoid Android: versatile protection for smartphones / Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), 2010, pp.347–356.
34. Choi E., Jeong H. User authentication using profiling in mobil cloud computing / AASRİ Confrence on Power and Energy Systems, 2012, pp.262–267.
35. Jia W., Zhu H., Cao Z., Wei L., Lin X. SDSM: a secure data service mechanism in mobile cloud computing / The First International Workshop on Security in Computers, Networking and Communications, 2011, pp.1087–1082.
36. Kim.T et al. Monitoring and detecting abnormal behavior in mobile cloud infrastructure / 2012 IEEE Network Operations and Management Symposium, 2012, pp.1303–1310.
37. Oberheide J., Veeraraghavan K., Cooke E., Jahanian F. Virtualized in-cloud security services for mobile devices / Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), 2008, pp.31–35.

**УДК 004.7**

**Алекперов Рашид Г., Алекперов Огтай Р.**
Институт Информационных Технологий НАНА, Баку, Азербайджан
rashid@iit.ab.az, oqtayalakbarov@yahoo.com

**Вопросы безопасности и конфиденциальности в мобильных облачных вычислениях**

В статье исследованы вопросы безопасности и конфиденциальности на облачных платформах, используемых в мобильных облачных вычислениях. Были проанализированы угрозы, возникающие для гарантированной защиты данных пользователей от внешних лиц и сетевой безопасности в мобильных облачных вычислениях. Кроме того, в статье были проанализированы информационная безопасность, конфиденциальность, размещение и перемещение данных, целостность информации, кибератаки и т.д. в мобильных облачных вычислениях. Были исследованы научно-теоретические проблемы безопасности и конфиденциальности мобильных облачных вычислений и проанализировано состояние научных исследований в этом направлении.

***Ключевые слова:*** *мобильные облачные вычисления, мобильное оборудование, информационная безопасность, конфиденциальность, кибератаки, вычислительные ресурсы, ресурсы памяти, облачные вычисления, виртуальная машина, облачные сервисы.*

**Rasid G.Alakbarov, Ogtay R. Alakbarov**
Institute of Information Technology of ANAS, Baku, Azerbaijan
rashid@iit.ab.az, oqtayalakbarov@yahoo.com

**Security and privacy issues in mobile cloud computing**

This article investigates security and privacy issues on cloud platforms used in mobile cloud computing. Threats arisen from users' data protection and network security in mobile cloud computing are analyzed. At the same time, the article analyzes information security in mobile cloud computing, confidentiality, location and displacement of data, completeness of data, cyber attacks.. Scientific-theoretical problems of security and privacy issues of mobile cloud computing are investigated and the status of researches in this direction is analyzed.

***Keywords:*** *mobile computing cloud, mobile equipment, information security, confidentiality, cyber attacks, computing and memory resources, computing clouds, virtual machine, cloud services.*