Mobil hesablama buludlarında təhlükəsizlik məsələləri

Rəşid Ələkbərov[1], Oqtay Ələkbərov[2]

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

[1]rashid@iit.ab.az; [2]oqtayalakbarov@yahoo.com

***Xülasə*— Məqalədə mobil hesablama buludlarında istifadə edilən bulud platformalarında təhlükəsizlik problemləri tədqiq edilmişdir. Mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkənin 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 analiz olunmuşdur.**

Açar sözlər*— *Mobil hesablama buludları, mobil avadanlıqlar, informasiya təhlükəsizliyi, konfidensiallıq, kiber hücumlar, hesablama və yaddaş resursları, hesablama buludları, virtual maşın, bulud xidmətləri

I. GIRIŞ

Hazırda dünyada hesablama buludları (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 yüksək sürətli əlaqə kanalına malik olan kompüter şəbəkələri əsasında yaradılır. Son dövrlərdə bulud texnologiyalarında yeni xidmətlərin və 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, smartfonlar və s.) istifadəsinin sürətlə artması və onların uyğun telekommunikasiya texnologiyalarının (GPS, 3G, 4G, Wi-Fi və s.) köməyi ilə internet üzərindən hesablama buludlarına qoşulması, yeni texnologiyanın – mobil hesablama buludları (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 ondan istifadə olunması hakerlər tərəfindən daha çox hücumlara məruz qalmasına və mobil istifadəçilərdə gizlilik problemlərinin yaranmasına səbəb olur. Bununla bağlı mobil qurğuların təhlükəsizliyinə təsir edən təhdidlər və mobil hesablama buludları sahəsindəki risklər araşdırılmışdır və tövsiyələr verilmişdir. Mobil hesablama mühitinin əsas məqsədi bulud xidməti provayderləri vasitəsi ilə internet üzərindən mobil istifadəçiləri proqram əlavələri və xidmətləri ilə təchiz etməkdir. Beləliklə, mobil hesablama buludlarında istifadəçilərin bulud serverlərdə yerləşmiş tətbiqi proqramlara əlyetərliliyini təmin etmək üçün şəbəkənin müxtəlif hissələrində: mobil qurğularda, şəbəkədə, mobil proqram əlavələrində təhlükəsizliklə əlaqədar problemləri analiz etmək vacibdir. Məqalədə mobil hesablama buludlarının istifadəsində meydana çıxan təhlükəsizlik və gizliliklə bağlı problemlər geniş şəkildə araşdırılmışdır.

II. MOBIL HESABLAMA BULUDU PLATFORMALARINDA 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 onları məlumatlarla təmin edir. Mobil hesablama buludlarında böyük hesablama və yaddaş resursları tələb edən verilənlər və proqram təminatı buludlarda yerinə yetirildiyindən, mobil qurğuların güclü texniki imkanlara malik olmasına ehtiyac duyulmur. İstifadəçilərin və müəssisələrin böyük həcmli məlumatlarının buludda yerləşdirilməsi və ondan istifadə olunması daha çox hakerlər tərəfindən hücumlara məruz qalmasına və mobil istifadəçilərdə gizlilik problemlərinin yaranmasına səbəb olur [1-2].

Hesablama buludlarında ənənəvi təhlükəsizlik məsələləri hələ də mövcuddur. Lakin müəssisənin imkanlarının və sərhədlərinin bulud xidmətlərindən istifadə edilməsi istiqamətində genişləndirilməsi ənənəvi təhlükəsizlik mexanizmlərinin buluddakı tətbiqi məlumatların konfidensiallığını 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

DOI: 10.25045/NCInfoSec.2017.05

təhlükəsizlik sərhədlərinə malik deyil. Bu təhlükəsizliyin pozulması halında təhlükəyə məruz qalan fiziki resursları təcrid etməkdə çətinliklər törədir;

- İstifadəçilərə 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 ehtiyacını 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 platformasında meydana çıxan problemlər. Bulud texnologiyalarında istifadəçiləri hesablama resursları ilə təmin etmək üçün bulud serverlərdə yaradılan virtual maşınlardan istifadə edirlər. Ona görə də **v**irtual maşınların (VM) təhlükəsizliyi əsas məsələlərdəndir. Ənənəvi təhlükəsizlik həllərindən istifadə edərək virtual maşınların 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) özlərinin təhlükəsizliyinə nəzarət vasitələrindən istifadə edərək gözlənən riskin səviyyəsini müəyyən edib, onu aradan qaldıra bilməlidir [5]:

- VM surətlərinin (image repository) saxlanması. Fiziki serverlərdən fərqli olaraq VM-lar avtonom rejimdə olduqda da risk altında olurlar. VM şablonları, VM-də yerləşən fayllara zərərli kodlarla təsir etməklə sıradan çıxarıla bilər və eyni zamanda onda olan məlumatları da oğurlanmaq mümkündür. VM şablonlarının etibarlı qorunması bulud provayderləri tərəfindən həyata keçirilir. VM şablonları ilə bağlı başqa bir məsələ, istifadəçinin ilkin məlumatları şablonlarda saxlana bilər və yeni istifadəçi isə bu şablonlardan istifadə etdikdə, qeyd edilən məlumatlardan istifadə etməklə gizlilik məsələlərini poza bilər;
- Virtual şəbəkə təhlükəsizliyi: Eyni şəbəkə infrastrukturundan yerləşən serverlərdən müxtəlif kirayəçilərin (arendator) birgə istifadə etməsi fiziki serverlərə və DNS-serverlərə müdaxilə ehtimalını artırır;
- Virtual maşınların sərhədlərinin təhlükəsizliyi: Virtual maşınlar fiziki serverlərlə müqayisədə virtual sərhədlərə malikdir. Bir fiziki serverdə yaradılan virtual maşınlar, eyni prosessordan, yaddaşdan, çıxış-giriş və şəbəkə adapterindən istifadə edirlər (VM resursları arasında heç bir fiziki təcridetmə yoxdur). VM-ın sərhədlərinin təmin edilməsində bulud provayderləri məsuliyyət daşıyır.

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

SaaS platformasında təhlükəsizlik məsələləri: SaaS modelində təhlükəsizliyin təmin edilməsi bulud xidmətləri və proqram təminatı 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 zəifliklərin tapılmasına imkan verməlidir.

Qeyd edilən təhlükələrin məqsədi istifadəçilərin şəxsi məlumatlarının (məs: kredit kartı nömrələri, parol, kimlərlə əlaqədə olması, yerləşmə yeri və s.) əldə edilməsi (oğurlanması) və ya onun mobil qurğusunun resurslarından istifadə etməsidir.

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.) üzləşir. Məsələn, GPS (Global Positioning System- Qlobal Yerləşmə Sistemi) texnologiyalarının proqram əlavələrindən istifadə etdikdə məlumatların konfidensiallığının qorunması ilə bağlı problemlər yaranır. Ona görə də mobil qurğuların təhlükəsizliyi üçün təhdidləri müəyyən edən təhlükəsizlik proqram təminatının yüklənməsi tövsiyə olunur. Şəbəkədə istifadə edilən müxtəlif mobil qurğularda təhlükəsizliyi təhdid edən zərərli proqramlar mobil istifadəçilərdə gizlilik məsələlərində problemlər yaradır. Mobil istifadəçilərin təhlükəsizliyi ilə bağlı iki əsas məsələ var: mobil əlavələrin təhlükəsizliyi və konfidensiallıq. Təhlükəsizlik problemlərinin yoxlanılmasının ən əsas üsulu mobil qurğularda təhlükəsizlik proqramını və antivirusun quraşdırılması və istifadəsi ilə həyata keçirilir. Mobil qurğuların resursları məhdud olduğu üçün təhdidlərdən qorunmaq fərdi kompüterlərə nəzərən daha çətin olur. Təhlükənin aşkarlanması və təhlükəsizlik mexanizmlərin 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 edir [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 təminatı vasitəsi ilə məlumatların oğurlanması;
- Proqram əlavələrin boşluğundan istifadə edərək məlumatların sızması məsələləri;
- Qurğuların və əməliyyat sistemlərinin daxilindəki boşluqdan;
- Təhlükəsiz şəbəkəyə giriş və etibarsız giriş nöqtələrinin olması;
- Təhlükəli bulud proqram əlavələrinin olması;
- Proqram əlavələri interfeyslərinin etibarlı idarə etmə imkanlarının olmaması.

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.

III. MOBIL HESABLAMA BULUDLARINDA TƏHLÜKƏSIZLIK VƏ GIZLILIK MƏSƏLƏLƏRI

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 edilir. SSL (Secure Sockets Layer) kriptoqrafik protokol olub, mobil istifadəçi ilə bulud server arasında əlaqə kanalında təhlükəsizliyi təmin edir [11]. Məlumatların təhlükəsiziliyi məsələsinə gəldikdə, şirkətlər məlumatların və əməliyyatların təhlükəsizlik siyasəti və prosedurlarını həyata keçirməlidir. Provayderlər siyasət və prosedurların tam yerinə yetirildiyinə əmin olmaq məqsədilə OPSEC (Open Platform for Secure Enterprise Connectivity - şəbəkəyə təhlükəsiz qoşulmaq üçün açıq platforma) haqqında istifadəcilərə ümumi şəkildə şirkət təlimləri, tədris və təlimatlar da keçirə bilər. 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 məlumatların və tətbiqlərin təhlükəsizliyini təmin olunması haqqında provayder tərəfindən istifadəçiyə zamənətin 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 [13,14]. İstənilən mobil qurğunun təhlükəsizlik problemlərinin aşkarlanmasının ən sadə yolu təhlükəsizlik proqram təminatının (Kaspersky, McAfee və AVG antivirus proqramları) onlarda quraşdırılması və istifadəsidir. Mobil qurğuların məhdud emal gücü və enerji təchizatı olduğuna görə onların təhlükələrdən qorunması digər kompüter qurğularına (məs., fərdi kompüter) nisbətən daha çətindir. Bunun üçün təhlükələrin aşkarlanması imkanlarını buluda köçürmək mümkündür.

Konfidensiallıq və gizlilik. Mobil istifadəçinin coğrafi yerinin aşkarlanması istifadəçinin vacib məlumatların (doğum tarixi, kredit kart məlumatları, şəxsi məlumatlar, xəstəlik tarixçəsi və s.) konfidensiallıq və gizlilik məsələlərinə dair problemlər yaradır [15]. Mobil qurğular GPS texnologiyasından istifadə edirsə, bu onun fiziki yerini təyin etməyi çox asanlaşdırır. Müəssisələrin məlumatlarının təhlükəsizlik məsələlərini yalnız müəyyən bulud xidmətlərinin analiz edilməsi vasitəsi ilə yüksəltmək olar. İstifadəçinin məlumatları bulud serverlərdə yerləşdirildikdən sonra, həmin məlumatlar 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 təminatların verilməsi və müvafiq qaydalar tətbiq edilməli, konfidensiallıq siyasəti və prosedurları istifadəçilərin məlumatının bulud serverlərdə təhlükəsizliyini təmin etməlidir. Məlumat və verilənləri toplayan şirkətlər onların təhlükəsiz emalı, saxlanması və yerləşdirilməsi üçün bəzi siyasət və prosedurlar qəbul etməli və onlara riayət 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 özlərini hüquqi və təhlükəsizlik problemlərindən qoruya bilər. Əks təqdirdə, onların informasiya infrastrukturu və reputasiyası ziyan görə bilər [16]. Məlumatların tamlığını və konfidensiallığını qorumağın ən effektiv yolu şifrləmədir. Şifrləmə məlumatların saxlanması və ötürülməsinə imkan verməklə əsasən onun emalını kənar müdaxilələrdən qoruyur [17,18]. Rəqəmsal hüquq idarə etməsi (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 təmin etmək və müəyyən məlumat toplularının (dəstlərinin) **harada** və hansı vəziyyətdə olduğunu təsvir etmək üçün müəyyən mexanizmlər həyata keçirməlidir. Bulud provayderi buludda xüsusi verilənlərin yerləşdirildiyi, onun mənşəyi və tamlıq mexanizmləri haqqında müştəriyə xəbərdarlıq etməlidir.

Məlumatların yerləşdirilməsi və yerdəyişməsi. Bulud verilənlərin yüksək mobilliyini təklif edir. İstehlakçılar öz məlumatlarının yerləşdiyi yeri hər zaman bilmir. 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 məlumatını qorunmasına görə məsuliyyət daşıyır.

Kiber hücumlar. Bütün şəbəkələr bir və ya bir neçə zərərli hücuma (haker) 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 (DoS - Denial of Service) hücumları.** Bulud serverləri daha çox DoS hücumalarına 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 virtual maşın 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 kanardan hücum edilir;
- ✓ **Autentifikasiya hücumları.** Virtual xidmətlər sahəsində autentifikasiya problemi ən zəif nöqtələrdən biri hesab olunur. İstifadəçi bədniyyətlilər 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 bədniyyətli (haker) özünü iki istifadəçi arasına salır. Bu növ hücumlarda bədniyyətli kommunikasiya yolunda yerləşir, daha sonra isə hər şey onun özündən asılı olur. Belə ki, o, rabitəyə müdaxilə edə və ya onu 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 məlumatların yayılması ilə əlaqədar siyasətə istifadəçilərin nə dərəcədə əməl etdiyini müəyyənləşdirə bilməz [23].

Uyğunluq və icra. Hazırda mobil hesablama buludların üçün heç bir formal standart siyasət toplusu mövcud deyil. Lakin Payment Card Industry Data Security Standard (PICDSS – Ödəniş Kartları Sənayesinin Verilənlərin Təhlükəsizlik Standartları), Health Insurance Portability and Accountability Act (HIPAA – Sağlamlıq Sığortasının Daşınarlığı və Hesabatlılığı Qanunu) standartlarında da verilənlərin saxlanması və istifadəsi üzrə bir sıra qaydalar mövcuddur [24]. Bu nizamnamələr üçün mütəmadi hesabat və auditin keçirilməsi tələb olunur. Korporativ verilənlərin buluda köçürülməsi üçün bu qaydalarının 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.

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 provayderi verilənlərin itməsi və sui-istifadəsinin qarşısını almaq və zərərli hücumlardan qorunmaq məqsədi ilə bəzi tədbirləri cəld şəkildə görmək üçün plan hazırlamalıdır. Əksər provayderlər onlara hücum edilə bilmədiyini iddia edərək, öz təhlükəsizlik xidmətlərini təkmilləşdir. 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. Digər sözlə desək, hər hansı hücumun qarşısının alınması onun sonradan bərpa edilməsindən daha asandır [25].

NƏTİCƏ

Məqalədə mobil hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və mobil hesablama buludları şəbəkəsinin təhlükəsizliyi məsələləri analiz olunmuşdur. Mobil hesablama buludlarının istifadəsi zamanı meydana çıxan təhlükəsizlik və məxfilik problemlər

araşdırılmışdır və həlli yolları göstərilmişdir. Məqalədə mobil hesablama buludlarında informasiya təhlükəsizliyi, konfidensiallıq, məlumatların yerləşdirilməsi və yerdəyişməsi, məlumatların tamlığı, kiber hücumlar və s. məsələlərdə geniş analiz olunmuşdur.

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] M.R. Gayathri, K. Srinivas, “A Survey on Mobile Cloud Computing Architecture, Applications and Challenges,” International Journal of Scientific Research Engineering & Technology, vol 3, no. 6, 2014, pp.1013-1021.

[2] R.Q. Ələkbərov, O.R. Ələkbərov, “Mobil hesablama buludları: mövcud vəziyyəti, axitekturası və problemləri,” İnformasiya Texnologiyaları Problemləri, vol 1, 2017. pp.42-52.

[3] Z. Xiao, Y. Xiao, “Security and Privacy in Cloud Computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, 2013, pp. 843-859.

[4] M. Gopichand, “An Overview of Security and Privacy Issue in Mobil Cloud Computing Environment,” International Journal of Advanced Researc in Computer Science and Software Engineering, vol. 6, no. 5, 2016, pp. 779-784.

[5] F.C. Abdullayeva, “Cloud kompyutinq mühitində təhlükəsizlik problemlərinin analizi,” Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları,II Respublika Elmi Konfransı, 2012, pp. 160-162.

[6] R. Caytiles, S. Lee, “Security considerations for Public Mobile Cloud Computing,” International Journal of Advanced Science and Technology, vol. 44, 2012, pp. 81-88.

[7] Y. Chen, V. Paxson, R.H. Katz , “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] Y.J. Chen, L.C. Wang, “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] S. Subashini, V. Kavitha, “A survey on security issues in service deliverymodels of cloud computing,” Journal of Network and Computer Applications, 2011, vol. 34, pp. 1-11.

[10] N. Fernando, L.W. Seng, L. Rahayu, “Mobile Cloud Computing: A Survey,” Journal of Future Generation System, Vol 29, No.1, 2013, pp. 84-106.

[11] A. Donald, S. Oli, L. Arockiam, “Mobile cloud security issues and challenges: A perspective,” International Journal of Engineering and Innovative Technology, vol. 3, no. 1, 2013, pp. 401.

[12] M. Sarrab, “Mobile Cloud Computing: Security Issues and Considerations,” Journal of Advances in Information Technology, vol. 6, no. 4, 2015, pp. 248-251.

[13] R. Collings, “Mobile Cloud Adoption Challenges in the Enterprise,” http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise/

[14] H.T. Dinh, C. Lee, D. Niyato, P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Communications and Mobile Computing. vol. 13, no. 18, 2013, pp. 1587-1611.

[15] A. Bahar, A. Habib, M. Islam, “Security architecture for mobile cloud computing,” International Journal of Scientific Knowledge Computing and Information Technology, vol. 3, no. 3, 2013, pp. 11-17.

[16] K.H. Jashizume, D. Rosado, E. Fernandez-Medina, B. Eduardo, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, vol. 4, no. 5, 2013, pp. 1-13.

[17] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, D. Zeghlach, “Challenges for Cloud Networking Security,” 2nd International ICST Conference on Mobile Networks and Management, 2010, pp. 2-16.

[18] H. Zhangwei, X. Mingjun, “A Distributed Spatial Cloaking Protocol for Location Privacy,” Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, 2010, pp. 468.

[19] P. Zou, C. Wang, Z. Liu, D. Bao, “Phosphor: A Cloud Based DRM Scheme with Sim Card,” Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), 2010, pp. 459.

[20] Y. Zhu, H. Hu, J. Ahn G., D. Huang, S. Wang, “Towards temporal access control in cloud computing,” INFOCOM, 2012, pp. 2576-2580.

[21] I. Lakshmi, “A Review on Cloud Computing in Mobile Applications,” International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, 2016, pp.149-161.

[22] M. Gregg, “10 Security Concerns for Cloud Computing,” Global Knowledge, 2010, pp. 2-7.

[23] M. Sarrab, H. Janicke, “Runtime monitoring and controlling of information flow,” International Journal of Computer Science and Information Security, vol. 8, no. 9, 2010, pp. 37-45.

[24] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, Z. Song, “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] D. Huang, Z. Zhou, L. Xu, T. Xing, Y. Zhong “Secure data processing framework for mobilecloud computing,” Proceeding IEEE INFOCOM Workshop on Cloud Computing, (INFOCOM’11), 2011, pp. 620-624.

SECURITY ISSUES IN MOBILE CLOUD COMPUTING

Rashid Alakbarov[1], Oqtay Alakbarov[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]*rashid@iit.ab.az*; [2]*oqtayalakbarov@yahoo.com*

Abstract – The article investigates security problems on cloud platforms used in mobile cloud computing. In mobile cloud computing, threats arising from guaranteed protection of user data from outsiders and network security are analyzed. At the same time, information security in mobile cloud computing, confidentiality, location and displacement of data, completeness of information, cyber-attacks, and so on are widely analyzed in the article.

Keywords – mobile cloud computing, mobile equipment, information security, confidentiality, cyber-attacks, computing and memory resources, cloud computing, virtual machine, cloud services.