Buludlarda fərdi məlumatların konfidensiallığına yönəlmiş hücumlar və müdafiə mexanizmləri

Fərqanə Abdullayeva
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
a_farqana@mail.ru

Xülasə— **Bulud texnologiyalarının təhlükəsizliyi buludda saxlanan verilənlərin konfidensiallığının pozulması ilə sıx əlaqədardır. Bulud texnologiyalarının heterogenlik, resursların paylaşılması, çoxicarəçilik, virtuallaşma, mobil bulud texnologiyaları, servis səviyyəsi müqaviləsi kimi xarakteristikaları bulud texnologiyalarında çoxsaylı boşluqlar yaradır. Məqalədə buludlarda saxlanan fərdi məlumatların konfidensiallığının pozulmasına yönəlmiş hücumlar və onların qarşısının alınması üsulları analiz olunur, bu hücumların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşıdurma tədbirlərinin qarşılıqlı əlaqə modeli təklif olunur.**

Açar sözlər— bulud texnologiyaları; fərdi məlumatlar; konfidensiallıq hücumları; anonimləşdirmə; verilənlərin manipulyasiyası hücümü

I. GİRİŞ

Bulud texnologiyaları bulud istifadəçilərinə paylaşılan hesablama resursları toplusuna giriş imkanı verən arxitekturadır. Son illər Big Data, IoT, 5G, SDN və NFV əsaslı bulud proqram tətbiqlərinin meydana gəlməsi ilə bulud texnologiyalarındakı sürətli inkişaf istifadəçilərin bulud texnologiyalarına miqrasiyasını artırmışdır [1]. Lakin bulud texnologiyalarının arxitekturası təhlükəsizliyi hədəfə almadan layihələndirildiyi üçün buluda olan təhlükəsizlik insidentlərinin sayı hər il böyük sürətlə artmaqda davam edir. Bu gün bulud xidmətləri təqdim edən nəhəng servis provayderləri olan Amazon, Google, Microsoft və s. böyük həcmdə təhlükəsizlik insidentləri ilə qarşılaşırlar. Bu provayderlərin infrastrukturlarının statistik qiymətləndirilməsi zamanı 2009-cu illə müqayisədə 2011-ci ildə bulud insidentlərinin sayı iki dəfə artaraq 33 insidentdən 71 insidentə qədər yüksəlmişdir [2].

Bulud texnologiyaları bulud servis provayderlərini və istifadəçilərini bir sıra təhlükəsizlik təhdidləri ilə üz-üzə qoyur. Bu təhlükəsizlik təhdidlərinin növlərinin sayı böyük sürətlə artır [3]. Burada bu təhdidləri reallaşdıran hücumların təbiəti fərqlidir. Onlar həm bulud provayderlərini, həm də istifadəçiləri hədəfə ala bilirlər. Bu səbəbdən bulud sisteminin özü və istifadəçiləri üçün təhlükəsizlik başlıca problemlərdən biri hesab olunur.

2016-cı ildə Bulud Təhlükəsizlik Alyansının (Cloud Security Alliance, CSA) bulud texnologiyaları üçün müəyyən etdiyi xarakterik 12 təhdid növü sırasında [3] verilənlərin pozulması (ing., data breach) başlıca mövqelərdən birini tutur.

Generasiya, ötürülmə, istifadə, paylaşılma, saxlanma, arxivləşdirmə, ləğv edilmə verilənlərin həyat tsiklinin mərhələlərini təşkil edir [4]. Verilənlərin təhlükəsizliyi həyat tsiklinin hər bir mərhələsində təmin edilməlidir.

Bulud texnologiyalarının təhlükəsizlik məsələlərinin analizinə həsr olunmuş çox sayda tədqiqatlar aparılmışdır. [5]-də bulud texnologiyalarının kommunikasiya, hesablama və servis səviyyəsi laylarında təhlükəsizlik məsələlərinin analizi aparılmışdır. Verilənlərlə bağlı təhlükəsizlik məsələlərinin analizində verilənlərin təhlükəsizlik məsələləri ötürülən verilənlərin təhlükəsizliyi və saxlanan verilənlərin təhlükəsizliyi kimi iki qrupa bölünür. Burada verilənlərin konfidensiallığının təmin edilməsi məsələsinə yetərli diqqət ayrılmır, problemlər ümumi təsvir olunur. [6]-da bulud texnologiyalarının müxtəlif modellərinin verilənlərin pozulması ilə bağlı problemləri analiz olunur. [7]–də verilənlərin təhlükəsizliyinin CIA (Confidentiality, Integrity, Availability) triadası baxımından analizi aparılır. CIA-triadası məşhur olduğuna baxmayaraq, bu triada bulud kimi dinamik mühitdə meydana çıxan yeni növ təhdidləri nəzərə ala bilmir [8]. Bu problemi aradan qaldırmaq üçün IAS-OCTAVE (Information, Assurance, Security) adı ilə tanınan kompleks təhlükəsizlik aspektləri siyahısı təklif edilmişdir [8]. Bu siyahıya görə hesabatlılıq, audit, autentiklik/etibarlılıq, əlçatanlıq, konfidensiallıq, tamlıq, inkar edilməzlik, məxfilik bulud texnologiyalarının informasiya təhlükəsizliyi aspektləri hesab olunur.

Məqalədə bulud texnologiyalarının çoxicarəçilik mühitində fərdi məlumatlarla bağlı təhlükəsizlik məsələləri analiz olunur, bu təhlükəsizlik problemlərinin aradan qaldırılması üçün mövcud metodlar təsvir olunur. Fərdi məlumatlara olan hücumların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşıdurma tədbirlərinin qarşılıqlı əlaqə modeli təklif olunur.

II. BULUD TEXNOLOGİYALARININ ƏSAS XARAKTERİSTİKALARI

Bulud texnologiyaları termini ilk dəfə 2006-cı ilin sonlarında Google şirkətinin icraçı direktoru Erik Şmid tərəfindən təklif edilmişdir.

Hazırda bulud texnologiyaları dördüncü sənaye inqilabının əsas komponentləri siyahısına daxil edilmişdir və qabaqcıl dünya dövlətlərində ən innovativ texnologiya hesab olunur [9].

DOI: 10.25045/NCInfoSec.2019.24

Bulud texnologiyaları verilənlər mərkəzinin resurslarını virtuallaşma texnologiyalarından istifadə etməklə paylaşan, o cümlədən müştərilərə elastik, tələbata uyğun, və ani servislər təqdim edən və istifadəçinin servis sərfiyyatını kommunal ödəniş kimi qiymətləndirən sistemdir [10].

Bulud texnologiyalarının əsas xarakteristikaları aşağıdakılardır [11, 12]:

- *Ölçülən servis* istifadəçiyə göstərilən servisin pul şəklində qiymətləndirilməsidir.
- *Ani elastiklik* resursların miqdarını çevik şəkildə artırıb-azaltmaq imkanının olmasıdır.
- *Sorğuya görə özünə xidmət* istifadəçinin bulud servisləri ilə sərbəst işləmək bacarığını göstərir.
- *Şəbəkəyə geniş giriş imkanı* buluda girişin təşkili istənilən məkandan, istənilən vaxt, istənilən qurğu vasitəsilə mümkün olmalıdır.
- *Resurslar toplusu* yaddaş, prosessor, hesablama resursları, şəbəkə resursları toplusudur.
- *Miqyaslaşma* resursların artımını idarə etmək imkanının olması.
- *Çoxicarəçilik* ayrı-ayrı müştərilərin seqmentləşdirilməsi, izolyasiyası, idarəetmə siyasətinin olmasının zəruriliyini göstərir.

III. BULUD TEXNOLOGİYALARININ TƏHLÜKƏSİZLİK STANDARTLARI

Bulud texnologiyalarının artıq bir çox yerlərdə tətbiq olunmağa başlaması bu sahədə çoxsaylı bulud standartlarının yaradılmasını zəruri etmişdir.

Provayder təşkilatlarında müvafiq idarəetmənin olduğunu ISO 2700X standartları seriyası vasitəsi ilə müəyyən edirlər. Bu standart aşağıdakıları müəyyən etməyə imkan verir:

- paylaşılan, çoxicarəçilik mühitdə müştərinin proqramlarının və verilənlərinin izolyasiya olunduğuna zəmanət;
- müştərinin aktivlərinin provayderin işçi heyəti tərəfindən icazəsiz girişdən qorunması;
- müştərinin aktivlərinin müştərinin işçiləri və ya partnyorları tərəfindən qəsdli və ya təsadüfi girişdən qorunması.

ISO təşkilatı ISO/IEC 27002 standartının üzərində bulud hesablama texnologiyaları üçün spesifik olan ISO/IEC 27017 standartını hazırlamışdır [13]. Bundan əlavə ISO/IEC 27001 standartının üzərində bulud xidmətlərinin təhlükəsizliyi və ümumi buludda fərdi məlumatların qorunması qaydalarını əks etdirən ISO/IEC 27018 standartını hazırlamışdır [14]. ISO/IEC 27036-4 bulud xidmətlərinin tətbiqi ilə bağlı spesifik informasiya təhlükəsizliyi riskləri və onların effektiv idarə edilməsi haqqında təlimat təqdim edir [15].

“ISO/IEC 19086 Cloud computing - Service level agreement (SLA) framework” fərdi məlumatların qorunması və təhlükəsizliyi qaydalarını müəyyən edir [16]. ISO/IEC 19086 (Part 4) buludun servis səviyyəsi haqqında müqavilələrinin təhlükəsizliyi və gizliliyi komponentləri ilə bağlı məsələləri əhatə edir [17]. ISO/IEC 27034 proqram tətbiqlərinin təhlükəsizliyi haqqında ümumi məlumat verilir. Proqram tətbiqlərinin təhlükəsizliyi ilə bağlı əsas anlayışlar, konsepsiyalar, prinsiplər və proseslər təsvir olunur. Bu standart layihələndirilən bütün növ infrastrukturlar üçün nəzərdə tutulmuş proqram tətbiqlərində istifadə oluna bilər [18]. NIST Special Publication 800-53 federal informasiya sistemlərinin təhlükəsizliyinin və gizliliyinin təmin edilməsi qaydalarını müəyyən edir [19]

Layihəçiləri təlimləndirmək məqsədi ilə OWASP-ın (Open Web Application Security Project) “OWASP Secure Coding Practices” adlı təhlükəsiz kodlaşdırma vərdişləri üçün təlimatları vardır [20]. Buludlarda fərdi məlumatların qorunmasına ITU (International Telecommunication Union) təşkilatı da böyük diqqət ayırır. Bu məqsədlə təşkilat “Privacy in Cloud Computing” adlı texniki sənəd dərc etdirmişdir [21]. Sənəddə buludlarda fərdi məlumatların konfidensiallığının pozulması risklərinin aradan qaldırılması üçün müxtəlif standartlaşdırma təşkilatları tərəfindən işlənəcək standartların problemləri analiz olunur. Bulud xidmətlərində fərdi məlumatların emalı ilə bağlı davranış kodeksləri vardır. Buna misal olaraq Avropa Birliyinin Bulud Davranış Kodeksini (EU Cloud Code of Conduct) misal göstərmək olar.

IV. BULUD TEXNOLOGİYALARININ İNFORMASİYA TƏHLÜKƏSİZLİYİ

İnformasiya təhlükəsizliyi informasiyanın və informasiya sisteminin icazəsiz girişdən, istifadədən, açıqlanmasından, pozulmasından, modifikasiya olunmasından, yoxlanmasından, yazılmasından, ləğv edilməsindən qorunmasıdır. CSA (Cloud Security Alliance) təşkilatının tədqiqatlarına görə bulud texnologiyalarının tətbiqi zamanı təşkilatlar aşağıdakı 12 təhdidlə qarşılaşa bilərlər [3]: verilənlərin pozulması, zəif identifikator, girişin və hesab verilənlərinin idarə edilməsi, mühafizəsis tətbiqi proqram interfeysləri, sistem və proqram tətbiqləri boşluqları, hesabın ələ keçirilməsi, zərərli insayderlər, təkmil davamlı hücumlar, verilənlərin itməsi, müvafiq araşdırmanın olmaması, bulud servislərindən ədalətsiz və sui-istifadə, xidmətdən imtina, paylaşılan texnologiya problemləri. Bundan əlavə bulud texnologiyaları üçün servislərin kənar mənbələrdən cəlb edilməsi, normativ qaydalara uyğunluq, verilənlərin yerləşmə məkanı, paylaşılan mühit, biznesin davamlılığı, qəza vəziyyətlərinin bərpası, qanunsuz fəaliyyətin təhqiqatı üçün çətin mühit, və uzun müddətli canlılıq kimi risklər də müəyyən edilmişdir [22].

Yuxarıda sadalanan təhdidlərin hamısı buludun resursları paylaşmaq və çoxicarəçilik xüsusiyyətinin olması səbəbindən baş verir və bu xüsusiyyətlər verilənlərin konfidensiallığının pozulmasına səbəb olan başlıca təhdidlərdir [23, 24].

V. BULUDLARDA İNFORMASİYANIN KONFİDENSİALLIĞININ POZULMASI

Buludlarda konfidensiallığın pozulmasına səbəb olan amillərdən biri buludların aparat təminatının ayrılmasının yetərli dərəcədə təmin edilməməsidir [25]. Buludda verilənlərin qalıcılığı (ing., data remanance) əlamətindən istifadə etməklə də konfidensiallığın pozulması halları baş verir. Burada müştəri bulud provayderindən yaddaş fəzası əldə edərək başqa müştərilərin həssas verilənlərini skanlama vasitəsi ilə axtarmaqla əldə edə bilir. Verilənlər üzərində idarəetmənin (ing., data governance) üçüncü tərəf buluda həvalə edilməsi də verilənlərin ələ keçirilməsi riskini artırır. Burada kənardan cəlb edilmiş servislər (bulud provayderi) müştərinin fərdi, məntiqi və fiziki təhlükəsizliyinin idarə edilməsi səlahiyyətlərini ələ keçirir.

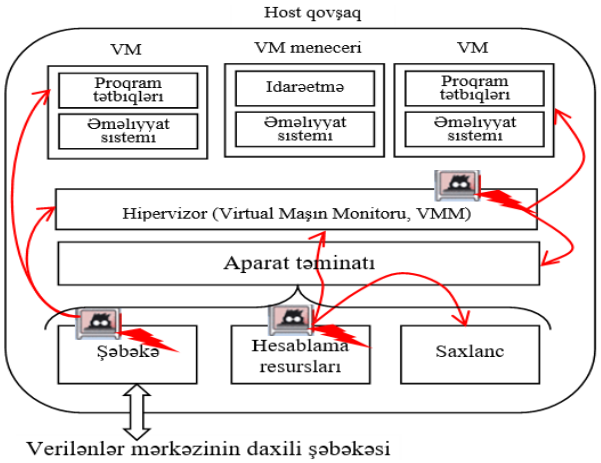
Fərdi məlumatların konfidensiallığı şəxsin özü haqqında verilənlərin saxlandığından məlumatlı olmaq, bu məlumatların necə əlaqələndirildiyinə nəzarət etmək və bu məlumatlardan sui-istifadənin qarşısını almaq səlahiyətinin olduğu deməkdir. Fərdi informasiyanın qorunması gizliliyə hüququn olması kimi təyin edilir. Hər bir şəxs tipindən asılı olmadan, gizli, açıq və ya peşəkar verilənlərini idarə etmək hüququna malikdir [21]. Bulud istifadəçilərinin buluda miqrasiya zamanı idarəetmə səlahiyyətini itirməsi verilənlərin tamlığı, konfidensiallığı və gizliliyi prinsiplərinə ciddi təhdid yaradır.

VI. BULUD SİSTEMİNİN BOŞLUQLARI

Hər bir bulud sistemi üç əsas komponentdən ibarətdir [26]: şəbəkə; hipervizor; aparat təminatı. Şəkil 1-də bulud sistemi və onun hücum nöqtələri təsvir olunmuşdur.

Koppalino bu sistemlərə xas olan üç hücum nöqtəsi müəyyən etmişdir [26]:

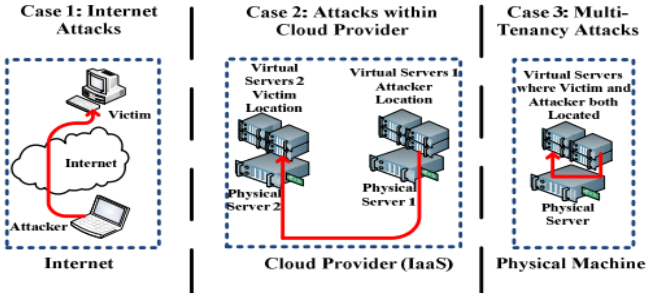
- *Bulud infrastrukturuna şəbəkə vasitəsi ilə hücumların daxil edilməsi.* Hücumlar xaricdən olan istifadəçilər vasitəsi ilə həyata keçirilir, onlar rabitə kanallarına təsir göstərməklə verilənlərin konfidensiallığını və tamlığını, bulud provayderinin verilənlər mərkəzinin əlçatanlığını pozamağa cəhd edirlər.
- *Hipervizordan istifadə etməklə digər virtual maşınlara hücumların edilməsi.* Hücumlar daxili istifadəçilər (virtual maşın (VM) sahibləri) tərəfindən edilir. Bu hücumun baş verməsinə başlıca səbəb buludun çoxicarəçilik xarakteristikasıdır (hücumçu və hədəf obyektin eyni hostda yerləşməsi faktı). Buludun bu komponentinə olan hücum müxtəlif proqram tətbiqləri arasında izolyasiyanın zəif qurulması səbəbindən baş verə bilir. Bu hücum həssas informasiyanın konfidensiallığının pozulmasına səbəb olur. Bu hücum növünü ənənəvi şəbəkə hücumlarının qarşısının alınması mexanizmləri vasitəsi ilə aradan qaldırmaq mümkün olmur.
- *Provayderin özünün hücumlar həyata keçirməsi.* İşçi heyətin aparat platformasında fiziki və ya məntiqi dəyişiklik etməklə istifadəçilərin həssas informasiyasın ələ keçirməsidir.



Şəkil 1. Bulud sisteminin hücum nöqtələri

VII. BULUDLARDA HÜCUM SSENARİLƏRİ

Buludlarda çoxicarəçilik riskinin unikallığı odur ki, burada hücumçular və hücum obyekti eyni serveri (fiziki maşın) paylaşaraq istifadə edir [23]. Belə hücum ənənəvi təhlükəsizlik mexanizmləri vasitəsi ilə aradan qaldırıla bilmir, çünki ənənəvi mexanizmlər serverin daxilinə nüfuz edə bilmir, və onların (ənənəvi mexanizmlər) monitorinq üsulları yalnız şəbəkə layı üçün layihələndirilmişdir. Hücumçu və hücum obyektinin müxtəlif yerləşmə ssenariləri şəkil 2-də təsvir edilmişdir.



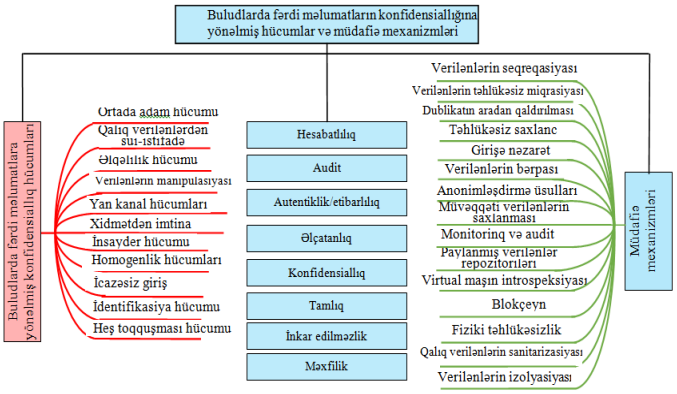
Şəkil 2. Ənənəvi şəbəkələşmə ilə bulud şəbəkələşməsi arasında fərq

Birinci halda hücumçu və hücum obyekti adi internet istifadəçiləridir. Bu tip hücumların qarşısının alınması üçün ənənəvi şəbəkə təhlükəsizliyi mexanizmləri yetərli hesab olunur. İkinci halda hücumçu və hücum obyekti eyni bulud provayderinin müştəriləridir, lakin onların hər biri ayrı-ayrı serverlərdə yerləşirlər. Bu struktur bulud texnologiyaları modelindəki virtuallaşmanın köməyi ilə qurula bilir. Bu tip strukturun təhlükəsizliyinin təmin edilməsi üçün bulud provayderi tərəfindən virtual şəbəkə təhlükəsizliyi mexanizmlərinin istifadə edilməsi lazım gəlir. Üçüncü halda hücumçu və hücum obyekti hər ikisi eyni buludun müştəriləridir və eyni serveri paylaşaraq istifadə edir. Bu hal buludun çoxicarəçilik xarakteristikasına görə yaradıla bilir. Burada hücumçunun virtual maşını ilə hucum obyektinin virtual maşını arasında şəbəkə kommunikasiyası bir fiziki maşının daxilində yaranır və onun mühafizə edilməsi sadə məsələ hesab olunmur. Burada trafik fiziki maşından kənara çıxmadığı üçün bu şəbəkəni ikinci halda olduğu kimi virtual

şəbəkə təhlükəsizliyi mexanizmləri vasitəsi ilə aradan qaldırmaq çətin olur.

VIII. BULUDLARDA FƏRDİ MƏLUMATLARIN KONFİDENSİALLIĞINA YÖNƏLMİŞ HÜCUMLARI VƏ MÜDAFİƏ MEXANİZMLƏRİ

Buludlarda fərdi məlumatların konfidensiallığına yönəlmiş hücumları, onların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşıdurma tədbirlərinin qarşılıqlı əlaqə modeli şəkil 3-də təsvir edilmişdir.



Şəkil 3. Buludlarda fərdi məlumatların konfidensiallığına yönəlmiş hücumlar və müdafiə mexanizmləri

- *Qalıq verilənlərdən sui-istifadə hücumu.* Bu hücum növündə hücumçunun fiziki saxlancı tam idarə etmək və ona giriş imkanı olduğu üçün təhlükəsizlik aspektlərinin hamısını birbaşa poza bilir.
- *Əlqəlilik hücumu.* Müxtəlif verilənlər mənbələrini ələ keçirmək və dolayı əlaqələndirməklə verilənlərin hissələrlə identifikasiyasını həyata keçirir. Burada hücumçu bulud verilənlərinə birbaşa müdaxilə etmədən ələ keçirilmiş verilənləri manipulyasiya etdiyi üçün bu hücum növü yalnız konfidensiallığın, tamlığın və məxfiliyin pozulmasına səbəb olur.
- *Verilənlərin manipulasiyası hücumu.* İstifadəçilər öz proqram tətbiqi komponentindən serverin proqram tətbiqi komponentinə göndərilən verilənlərdə dəyişikliklər etməklə veb-proqram tətbiqlərinə hücum edir. Başqa sözlə, server komponentinin qəbul etdiyi giriş verilənləri müştərinin daxil etdiyi gözlənilən verilənlər olmur, tam dəyişdirilmiş verilənlər olur. Burada hücumçu bulud verilənlərinə birbaşa müdaxilə edə bildiyi üçün verilənlərin manipulasiyası hücumu bütün təhlükəsizlik aspektlərini poza bilir.
- *Yan kanal hücumları.* Yan kanal aparat təminatındakı gizli kanaldır. Yan kanal məlumatlarından istifadə edən istənilən növ hücum yan kanal hücumu adlanır. Bu hücum verilənlərin tamlığını, konfidensiallığını və məxfiliyini pozur.
- *Xidmətdən imtina.* Bulud servis provayderlərinin xidmət təqdim etmək prosesini dayandıran hücumlardır.
- *Homogenlik hücumları.* Hücumçu dolayı yolla fərdi məlumatları xüsusi identifikatorlara aid edə bilir. Bu hücum verilənlərin tamlığını, konfidensiallığını və gizliliyini pozur.
- *İcazəsiz giriş hücumu.* Müştərilərin verilənləri buludda saxlandıqda onların verilənlər üzərində nəzarət hüququ itir. Bulud texnologiyalarında verilənlər müxtəlif ölkələrdə yerləşmiş çoxsaylı verilənlər mərkəzlərində saxlana bilər. Belə ölkələr verilənlərin sahibindən icazə almadan verilənlərə giriş etmək üçün daha üstün səlahiyyətə malik olur. VM-lərin etibarsız hosta miqrasiyası zamanı hücumçu bulud verilənlərinə icazəsiz giriş əldə edə bilər. Bu zaman hücumçu həmin virtual maşındakı həssas məlumatı açıqlaya bilər. Bu hücum növü informasiya təhlükəsizliyi aspektlərinin hamısını birbaşa poza bilir.
- *İdentifikasiya hücumu.* Hücumçu bəzi identifikasiya atributlarını (ad, ünvan) müəyyən şəxslə əlaqələndirə bilir. Bu hücum növü yalnız konfidensiallığın, tamlığın və məxfiliyin pozulmasına səbəb olur.
- *Heş toqquşması hücumu.* Hücumçunun məqsədi heş funksiyanın eyni heş qiyməti verən iki giriş simvolunu tapmaqdır.
- *Ortada adam hücumu.* Subyektlər arasında ötürülən informasiyanın ələ keçirilməsidir.

Yuxarıda sadalanan hücumların qarşısının alınması üçün müdafiə mexanizmləri kimi aşağıdakılar istifadə edilə bilər:

- *Dublikatın aradan qaldırılması.* Verilənlərin artıq nüsxələrinin sistemdən silinməsi prosesidir.
- *Təhlükəsiz saxlanc.* Müxtəlif şifrləmə üsullarından istifadə etməklə təhlükəsiz saxlancın qurulmasıdır.
- *Girişə nəzarət.* Buludda saxlanan verilənlərə olan girişin idarə edilməsi üsullarıdır.
- *Verilənlərin bərpası.* İtirilmiş verilənlərin bərpası prosesidir.
- *Anonimləşdirmə üsulları.* Verilənlərin anonimləşdirilməsini həyata keçirmək üçün k-anonymity, l-diversity, t-closeness anonimləşdirmə üsulları istifadə olunur.
- *Müvəqqəti verilənlərin saxlanması.* Bu tip verilənlər sessiya zamanı yaranan verilənlərdir. Verilənlərin saxlanması üsullarının işlənməsi məsələlərini əhatə edir.
- *Paylanmış verilənlər repozitoriləri.* Yeni təhlükəsiz saxlanc arxitekturalarının işlənməsidir.
- *Virtual maşınların introspeksiyası.* Tətbiq proqramın, qonaq əməliyyat sistemlərinin və fiziki serverdə işləyən VM-lərin vəziyyətinin monitorinqi üsullarıdır. Fərdi məlumatların saxlandığı virtual maşınların fəaliyyətini yoxlayır, virtual maşında zərərli proqramı aşkarlayır.

- *Blokçeyn.* Blokçeyn texnologiyasına əsaslanan şifrlənmiş verilənlər saxlancı sisteminin qurulması.
- *Monitorinq və audit.* Bulud saxlancının monitorinqi üçün miqyaslanan paylanmış sistemlərin işlənməsi.
- *Verilənlərin təhlükəsiz miqrasiyası.* Verilənlərin bir bulud saxlancından digərinə köçürülməsi.
- *Qalıq verilənlərin sanitarizasiyası.* Verilənlər həyat tsiklinin sonunda təhlükəsiz qaydada silinməlidir. Ənənəvi sanitarizasiya üsulu kimi üzərindən yazılma (overwriting) istifadə oluna bilər.
- *Verilənlərin izolyasiyası.* Həssas və adi verilənlər arasında bölünmənin olmasını nəzərdə tutur.
- *Verilənlərin seqreqasiyası.* Virtuallaşmış mühitdə bulud istifadəçiləri arasında tam bölünmənin olması.

NƏTİCƏ

Buludlarda saxlanan fərdi məlumatların təhlükəsizliyinin təmin edilməsinin müasir vəziyyəti analiz edilmiş, verilənlərin konfidensiallığına olan hücumlar müəyyənləşdirilmişdir. Bu hücumların aradan qaldırılması üçün bir sıra yanaşmalar təsvir edilmişdir. Müxtəlif istifadəçilərin verilənlərinin bir-birindən ayrılmasını təmin etmək üçün verilənlərin intellektual seqreqasiyası üsullarının işlənməsinin zəruriliyi qeyd edilmişdir.Verilənlərin sızması riskini aradan qaldırmaq üçün saxlanmış verilənlərin şifrlənməsinin vacibliyi göstərilmişdir.

İSTİNADLAR

[1] “Hosting and cloud computing market size worldwide 2010-2020,” 2018, https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

[2] “Cloud Computing Vulnerability Incidents: A Statistical Overview,” 2013, 22 p.

[3] K. Walker, “Cloud security alliance (CSA). The treacherous 12: cloud computing top threats in 2016,” https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/.

[4] D. Chen, H. Zhao, “Data security and privacy protection issues in cloud computing,” In proccedings of the international conference on computer science and electronics engineering, 2012, pp. 647-651.

[5] S. Nalini, A. Jeyaraj, “Recent security challenges in cloud computing,” Computers and Electrical Engineering, 2018, vol. 71, pp. 28–42.

[6] R.Barona, E.A. Anita, “A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats,” In proccedings of the international conference on circuits power and computing technologies, ICCPCT, 2017, pp. 1-8.

[7] P.R. Kumar, P.H. Raj, P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” Procedia Computer Science, 2018, vol. 125, pp. 691-697.

[8] Y. Cherdantseva, J. Hilton, “A reference model of information assurance and security,” In proccedings of the International Conference on Availability, Reliability and Security, ARES, 2013, Regensburg, Germany, 2–6 September , pp. 546–555.

[9] M.H. Onik, C.S. Kim, J. Yang, “Personal Data Privacy Challenges of the Fourth Industrial Revolution,” In proccedings of the international conference on advanced communications technology, (ICACT), 2019, pp. 635-638.

[10] M.T. Khorshed, A.B. Ali, S.A. Wasimi, “A Survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” Future Generation Computer Systems, 2012, vol. 28, no. 6, pp. 833-851.

[11] P. Mell, T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, 2009, 7 p.

[12] “Security Guidance for Critical Areas of Focus in Cloud Computing,” 2009, Cloud Security Alliance, V 2.1, 76 p.

[13] “ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” 2015, https://www.iso.org/standard/43757.html

[14] “ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” First edition 2014, 32 p.

[15] “ISO/IEC 27036-4, Information technology - Security techniques - Information security for supplier relationship - Part 4: Guidelines for security of cloud services,” 2016, First edition, 28 p.

[16] “ISO/IEC 19086, Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts,” 2016, First edition, 11 p.

[17] “ISO/IEC 19086 Cloud computing - Service level agreement (SLA) framework, Part 4, Components of Security and of protection PII,” 2019, 8 p.

[18] “ISO/IEC 27034, Information Technology- Security techniques,” Application Security, First edition, 11 p.

[19] “NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4, 2013, 462 p.

[20] “Open Web Application Security Project (OWASP),” https://www.owasp.org

[21] “Privacy in Cloud Computing,” ITU-T Technology Watch Report March 2012, 26 p.

[22] J. Brodkin, “Gartner: seven cloud-computing security risks,” July 02, 2008, https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html

[23] D. Zissis, D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, 2012, vol. 28, no. 3, pp. 583-592.

[24] Special Publication 800-144, “Guidelines on Security and Privacy in Public Cloud Computing,” NIST, 2011, 80 p.

[25] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, J. Xu, “Multi-Tenancy in Cloud Computing,” In proccedings of the 8th IEEE International Symposium on Service Oriented System Engineering, SOSE, 2014, pp. 344-351.

[26] L. Coppolino, S. D’Antonio, G. Mazzeo, L. Romano, “Cloud security: Emerging threats and current solutions,” Computers and Electrical Engineering, 2017, vol. 59, pp. 126-140.

PRIVACY ATTACKS IN CLOUDS AND PREVENTIVE MECHANIZMS

Fargana Abdullayeva

Institute of Information Technology of ANAS, Baku, Azerbaijan

a_farqana@mail.ru

Abstract − Cloud computing security is closely related to the breach of data privacy stored in the cloud. The characteristics of cloud computing such as heterogeneity, resource sharing, multitenancy, virtualization, mobile cloud computing, and service level agreement create numerous vulnerabilities in cloud technologies. In this paper privacy violation attacks to the data stored on the cloud and their preventive methods are analysed, a relational model of the impact of these attacks on the various security aspects of cloud computing and preventive methods is proposed.

Keywords **−** *cloud computing; personal data; privacy attack; anonymization; data manipulation attack*