Buludlarda fərdi məlumatlarin mühafizəsi problemləri

Rəşid Ələkbərov[1], Arzu Həsənli[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*rashid@iit.ab.az*, [2]*arzuhlee1@gmail.com*

***Xülasə* — Bulud texnologiyaları istifadəçilərin böyük hesablama və yaddaş resursları tələb edən məsələlərinin həllini təmin edən şəbəkə texnologiyasıdır. Bulud hesablama xidmətləri istifadəçinin məlumatlarını şəbəkə üzərindən bulud serverlərdə yerləşdirərək, məlumatların virtual maşınlar vasitəsilə emal edilməsinə imkan yaradır. Bu məlumat mərkəzləri dünyanın istənilən nöqtəsində istifadəçilərin əlyetərliyindən və nəzarətindən kənarda yerləşdiyindən, xidmətdən istifadə etdikdə çoxşaxəli təhlükəsizlik və məxfilik problemləri yaranır. Məqalədə buludlarda saxlanılan məlumatlara yönələn təhlükələr, təhdidlər, onlara qarşı mübarizə üsulları araşdırılmışdır.**

Açar sözlər – hesablama buludları, IaaS, PaaS, SaaS, bulud xidmətləri, məxfilik, təhlükəsizlik.

I. GİRİŞ

Hazırda bulud hesablaması İnternet sənayesinin ən aktual mövzularından biridir. Təşkilatlar və fərdi internet istifadəçiləri məlumatlarını saxlamaq və emal etmək üçün bulud hesablama texnologiyalarından geniş istifadə edirlər. Lakin buludda yerləşən məlumatların özü də bir sıra təhdidlərə məruz qala bilər və məlumatların məxfiliyi və bütövlüyü pozula bilər. Buludun xarici təhdidlərdən qorunması üçün müntəzəm olaraq yoxlanılması lazımdır. Fərdi istifadəçilərin və müəssisələrin böyük həcmli məlumatlarının buludda yerləşdirilməsi və ondan istifadə olunması hakerlər tərəfindən daha çox hücumlara məruz qalmasına və istifadəçilərdə məxfilik problemlərinin yaranmasına səbəb olur. Bulud serverlərdə məlumatların təhlükəsizliyinin və məxfiliyinin qorunması aktual məsələlərdəndir.

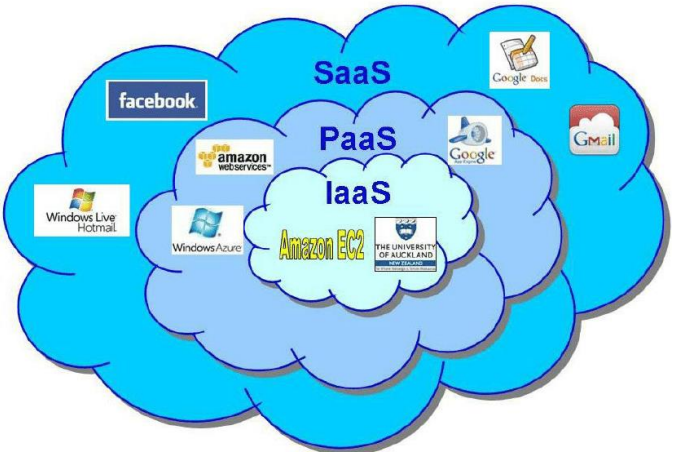
II. BULUD XİDMƏTLƏRİ

Hal-hazırda bulud texnologiyalarında ən çox istifadə olunan xidmətlər aşağıdakılardır (şəkil 1) [1]:

Infrastructure-as-a-service (IaaS) – infrastruktur servis kimi. IaaS səviyyəsi infrastrukturun icarəyə götürülməsi servisini həyata keçirməyə imkan verir.

Platform-as-a-service (PaaS) – platforma servis kimi. PaaS servisi istifadəçilərə virtual serverlərdə yerləşən əməliyyat sistemlərindən və xüsusiləşdirilmiş proqram əlavələrindən istifadə etməyə imkan yaradan virtual platformadır.

Software-as-a-service (SaaS) – proqram təminatı servis kimi. İstifadəçiləri proqram təminatı ilə təmin edir. İstifadəçi proqram təminatını almır və lazım gələndə ondan məsələnin həllində istifadə edir və istifadəyə görə uyğun məbləği ödəyir.



Şəkil 1. Hesablama buludlarının modeli

Hesablama buludları aşağıdakı üstünlüklərə malikdir [2]:

- İnternetə qoşulan fərdi kompüterlərin hesablama və yaddaş resurslarına olan tələbatını azaldır;
- istifadəçilərin məhdudiyyətsiz hesablama və yaddaş resursları ilə təmin olunmasına imkan verir;
- hesablama və yaddaş resurslarından faktiki istifadəyə görə təminatçıya ödəniş olunur;
- verilənlərin yüksək sürətlə emalı həyata keçirilir;
- aparat və proqram təminatına, xidmətə və elektrik enerjisinə olan xərclər azalır;
- istifadə olunan proqramlar daim yenilənir və s.

Bulud texnologiyalarında istifadəçilərin proqram əlavələri və fərdi məlumatları onların fərdi kompüterlərində yox, əsasən İnternet şəbəkəsinin bulud serverlərində yerləşdirilir. İstifadəçilərin göndərdiyi sorğulara uyğun olaraq onları əldə etmək istədikləri məlumatlarla təmin edir. Hesablama buludlarında ənənəvi təhlükəsizlik məsələləri hələ də mövcuddur. Bulud xidmətləri təklif edən provayderlər müştərilərinə yaxşı xidmət göstərmək üçün zaman-zaman yeni imkanlar təklif edir. Təqdim edilən yeni və daha mürəkkəb əlavələr ənənəvi təhlükəsizlik mexanizmlərinin buluddakı məlumatların məxfiliyini tam təmin edə bilməməsinə səbəb olur. Buludların açıqlığı və çoxsaylı xidmətlərin xüsusiyyətləri

DOI: 10.25045/NCInfoSec.2019.07

hesablama buludlarının informasiya təhlükəsizliyinin təmin edilməsində problemlər yaradır [3,4]:

- Bulud platformalarında istifadə olunan proqram əlavələri və saxlanan məlumatlar sabit infrastruktur və təhlükəsizlik sərhədlərinə malik deyil. Bu isə buludda təhlükəsizliyin pozulması hallarında fiziki resursların sistemdən təcrid edilməsində çətinliklərə səbəb olur;
- İstifadəçilərə bulud xidmətləri təklif edən bulud platformalarının çoxsaylı provayderlərə məxsus olması buludda mübahisəli hadisə baş verdikdə, onun həllinə vahid təhlükəsizlik tədbirləri tətbiq etməyi çətinləşdirir;
- Buludun açıqlığı və çoxsaylı istifadəçilərin bulud serverlərdən istifadəsi, icazəsi olmayan şəxslərin istifadəçilərin məlumatlarına giriş əldə etməsinə imkan yaradır;

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

Potensial hücumlara aşağıdakılar aid ola bilər [5]:

- bulud serverlərə müdaxilə;
- kanala kənar hücumlar;
- autentifikasiya hücumları;
- şəxs vasitəsilə şifrləmə hücumları və s.

Bulud xidmətlərində müxtəlif təhlükəsizlik məsələlərini: məxfilik, məlumatın tamlığı, bərpası və istifadəçi məlumatlarının idarə edilməsi, məlumat təhlükəsizliyini təmin etmək üçün aşağıdakı prosedur qaydalar tətbiq edilməlidir:

Məlumat təhlükəsizliyini təmin etmək üçün təhlükəsizlik standartlarını şifrələmə metodlarından istifadə edilməlidir.

Xidmət təminatçılarının (provayderlərin) istifadəçi məlumatlarına əlçatanlığı məhdud olmalıdır, onlar məlumatlara müdaxilə edə bilməməlidirlər.

Şəbəkəni idarə edən serverlərə icazəsiz və qanunsuz girişin qarşısını almaq üçün sərt giriş protokolları tətbiq olunmalıdır.

İstifadəçi məlumatlarının ehtiyat nüsxələri yaradılmalıdır ki, qəza baş verdikdə onları bərpa etmək mümkün olsun.

III. BULUD TEXNOLOGİYASINDAKI BARYERLƏR VƏ TƏHLÜKƏSİZLİK TƏHDİDLƏRİ

Hal-hazırda bulud texnologiyasından geniş istifadə edilməsinə baxmayaraq, bir çox təşkilatlar bulud xidmətlərinin təhlükəsizliyinin təmin edilməsindən cox narahatdır. Sistemin arxitekturasındakı bəzi boşluqlar bulud hesablamasını müxtəlif təhlükəsizlik və məxfilik təhdidlərinə qarşı müdafiəsiz etmişdir. Bu keçid konsepsiyasının sərhədlərini məhdudlaşdıran aşağıdakı məsələlərdir[6-8]:

Məxfilik və təhlükəsizlik – hər hansı bir yeni hesablama texnologiyasının müvəffəqiyyətini təyin edən əsas amil onun etibarlı olduğu müddətə əsaslanır. Fərdlərin məlumatlarının hesablama buludlarında bulud serverlərində saxlanması təhlükəsizlik və məxfilik baxımından fərdi kompüterlərin məlumat daşıyıcılarında saxlanmasına nəzərən daha az etibarlıdır. Fərdi kompüterlərdə saxlanılan məlumatları istənilən zaman sabit disklərə və sistemlərə daxil olmaqla əldə etmək mümkündür, ancaq bulud serverləri potensial olaraq dünyanın hər yerində yerləşə bilər və İnternetdə baş verən hər cür qəzalar buludda olan məlumatlara girişin qarşısını ala bilər.

Performans, gecikmə və etibarlılıq. İstifadəçi və bulud serverləri arasında məlumat mübadiləsində gecikmələr və etibarlılıq məsələləri bulud hesablamalarında problemlərə səbəb olmuşdur. Gecikməni artıran digər amillər məlumatların etibarsız və ictimai şəbəkələrdə (hər kəsin, yəni ümumi kütlənin daxil olduğu və digər şəbəkələrə və ya İnternetə qoşula biləcəyi bir şəbəkədir) hərəkəti zamanı tıxanma, küy və paket itkisi ilə müşayiət olunan şifrələmə və deşifrələmə prosesidir.

Portativlik. Bəzi hallarda təşkilatlar bulud təminatçılarını dəyişdirmələri lazım gəlir. Şirkətlər istifadə etdiklərindən daha yaxşı başqa bir bulud platformasını tapdıqları təqdirdə məlumatlarını və tətbiqlərini yeni platformaya köçürə bilmədikləri hallar yaşanmışdır. Bundan başqa, bəzi şirkətlər öz tələblərinə uyğun olaraq bulud xidməti təminatçıları tərəfindən təqdim olunan xidmətlərin müxtəlifliyinə görə fərqli tətbiqlər üçün fərqli bulud platformalarından istifadə edirlər. Bu səbəbdən bulud texnologiyalarında portativlik xüsusiyyəti həyati funksiya daşıyır.

Fiber optik şəbəkələr vasitəsi ilə məlumatların sızdırılması. Son bir neçə ildə tranzit məlumatların təhlükəsizlik risklərinin artdığı diqqəti cəlb edir. Məlumatların şəbəkə vasitəsilə ötürülməsi hazırda normal prosesdir və bir çox məlumat mərkəzləri ictimai və ya özəl bulud modelləri kimi digər bulud yerləşdirmə modellərini əhatə edə bilər. Son dövrlərdə bir məlumat mərkəzindən digərinə ötürülən məlumatların təhlükəsizliyinin pozulması faktlarına daha çox rast gəlinib.

IP şəbəkələri üzərində məlumatların saxlanması. İnternet məlumatların saxlanması hal-hazırda olduqca populyarlaşır və yaxın illərdə müəssisələrin verilənləri saxladığı sistemlərinin əksəriyyətinin şəbəkəyə qoşulacağı müşahidə edilmişdir, çünki bu, müəssisələrə tələb olunan arxitekturanı qurmadan çox böyük məlumat toplamağa imkan verir. Onlayn məlumat saxlamağın bir çox üstünlükləri olsa da, buludda vacib məlumatların sızmasına və ya məlumatların əlçatmazlığına səbəb ola biləcək təhlükəsizlik təhdidləri mövcuddur.

Aşağıda buludlara qarşı yönələn müxtəlif təhlükəsizlik təhdidləri və hücumları göstərilmişdir[9,10,11]:

- SQL injection;
- Cross-Site Scripting (XSS) hücumları;
- DoS hücumları;
- DDoS hücumları;
- Google Hacking;
- Forced Hacking.

Göstərilən hücumları aşkar etmək üçün bir neçə standart üsullardan istifadə edirlər: Kodda dinamik olaraq yaradılan SQL-in istifadəsinin qarşısını almaq, kodda istifadə olunan meta quruluşlarını tapmaq, istifadəçinin daxil etdiyi bütün parametrləri təsdiqləmək, lazımsız məlumatların və simvolların qəbul edilməməsi və silinməsi və s. Ümumi təhlükəsizlik çərçivəsində meyarlar müəyyən olunmalı, hər hansı bir bulud mühiti ilə əlaqə qurmaq üçün xüsusi hazırlanmış və əvvəlcədən təyin edilmiş təhlükəsizlik siyasəti tətbiq edilməli və prosesin sonrakı mərhələləri də nəzarət altında saxlanılmalıdır.

Bənzər bir yanaşma, İnternetdən gələn təhlükəsizlik təhdidlərini bloklayan və şəbəkəyə çatmadan məlumatları süzgəcdən keçirən Symantec Mesaj Labs Web Security proqram təminatından bulud serverlərində geniş istifadə olunur. Buludlarda yaradılan Veb səhifələrin təhlükəsizliyinin təmin edilməsi iki komponentə əsaslanır [12, 13]:

Çox səviyyəli təhlükəsizlik – məlumat təhlükəsizliyini təmin etmək və mümkün zərərlərin qarşısını almaq üçün çox səviyyəli təhlükəsizlik platformasından ibarətdir.

URL-lərin süzülməsi – əksər hallarda hücumlar müxtəlif veb səhifələr və İnternet saytları vasitəsilə də həyata keçirilir. URL-lərin süzülməsi veb-səhifələrin süzgəcdən keçirildiyi, veb-səhifənin zərərli və ya təhlükə daşıyan məlumata malik olub olmadığını yoxlayir. Bundan başqa, arzuolunmaz saytların məzmununu da bloklaya bilər. Eyni zamanda URL-lərin süzülməsi çevik texnologiya olub, sistemin çox ziddiyyətli mühitlərində də təhlükəsizliyi təmin edir və yeni və yaxınlaşan zərərli proqram təhlükələrindən qoruyur.

NƏTİCƏ

Məqalədə hesablama buludlarında istifadə edilən bulud platformalarda təhlükəsizlik problemlər tədqiq edilmişdir. Hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkənin təhlükəsizliyi istiqamətində meydana çıxan təhdidlər analiz və təhlil olunmuşdur, hesablama buludlarının istifadəsi zamanı meydana çıxan təhlükəsizlik və məxfilik problemləri araşdırılmışdır və həlli yolları göstərilmişdir.

İSTİNADLAR

[1] R.Q. Ələkbərov, M.A. Həşimov “Bulud texnologiyaları: xidmətlər, problemlər və tətbiq sahələri”, İnformasiya texnologiyaları problemləri, 2016, №1, s.3–10.

[2] O.R. Ələkbərov “Mobil hesablama buludlarında təhlükəsizlik və konfidensiallıq məsələləri”, İnformasiya texnologiyaları problemləri, 2018, №1, s.92-103.

[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] K.Hashizume, D.G. Rosado, E. F. Medina, E. B Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013.

[6] P.K.Tiwari1, B.Mishra, “Cloud computing security issues, challenges and solution”, International Journal of Emerging Technology and Advanced Engineering, Vol 2, Issue 8, August 2012.

[7] A. Ansari and Ch. Bawankar, “Privacy & data integrity for secure cloud storage”, IOSR Journal of Computer Science, 2014.

[8] R.Bhadauria, R.Chaki, N. Chaki, S. Sanyal “A survey on security issues in cloud computing,” arXiv preprint arXiv:1109.5388, pp. 1-15, 2011.

[9] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud security issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009.

[10] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, “Resource allocation for security services in mobile cloud computing,” in Proc. IEEE INFOCOM’11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, 2011.

[11] W. Li, L. Ping, X. Pan, “Use trust management module to achieve effective security mechanisms in cloud environment,” 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14-19, 2010.

[12] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”; Journal of Network and Computer Applications, Vol. 34(1), pp. 1–11, 2011.

[13] L. Wang, G. Laszewski, M. Kunze, J. Tao, “Cloud computing: A perspective study”, New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008.

PROBLEMS OF PERSONAL DATA PROTECTION IN CLOUDS

Rashid Alekperov[1], Arzu Hasanli[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]rashid@iit.ab.az, [2]arzuhlee1@gmail.com

Abstract – Cloud technology is a network technology that enables users to solve issues that require large computing and memory resources. Cloud computing services enable the processing of data through virtual machines, placing user data across the network on cloud servers. As these data centers are located anywhere in the world away from the direct access and control of users , the use of the service creates a multitude of security and privacy concerns. The article explores the dangers, threats, and methods for combating of information stored in clouds.

Keywords– *computing technologies, IaaS, PaaS, SaaS, cloud services, cloud computing, privacy, security*