

Fəxri Məmmədov
Azərbaycan Memarlıq və İnşaat Universiteti
Magistrant
<https://orcid.org/0009-0007-3287-2881>
fakhriM@risk.az

Bulud texnologiyalarının informasiya texnologiyalarında rolu və müəssisə sistemlərinin rəqəmsal transformasiyasında tətbiqi

Xülasə

Bulud texnologiyaları müəssisələrin rəqəmsal transformasiyasını sürətləndirir. Bu texnologiya resursların internet üzərindən çevik istifadəsini, xərclərin optimallaşdırılmasını və xidmətlərin davamlılığını təmin edir. Məqalədə buludun xidmət modelləri, təhlükəsizlik məsələləri və müəssisələrə təsiri araşdırılmışdır.

Tədqiqat göstərir ki, bulud texnologiyalarının tətbiqi yalnız texniki keçid deyil, həm də təhlükəsizlik, idarəetmə və maliyyə nəzarəti ilə bağlı kompleks prosesdir.

Açar sözlər: *bulud texnologiyası, rəqəmsal transformasiya, IaaS, PaaS, SaaS, kibertəhlükəsizlik, FinOps, hibrid bulud, DevOps*

Giriş

XXI əsrdə rəqəmsallaşma, süni intellekt və böyük verilənlər daha çevik texnoloji mühitə ehtiyacı artırmışdır. Bu ehtiyacların qarşılanmasında bulud texnologiyaları mühüm rol oynayır. Bulud texnologiyası server, saxlama və proqram təminatı kimi resursların internet üzərindən xidmət formasında istifadəsinə imkan verir [1].

Bulud texnologiyaları resursların elastik idarə olunmasını təmin edir və müəssisələrə daha sürətli, çevik və avtomatlaşdırılmış idarəetmə imkanı yaradır. Bu yanaşma innovasiya sürətini və bazar tələblərinə uyğunlaşmanı artırır.

Bu gün bulud texnologiyaları biznes, təhsil, bank və dövlət sektorunda geniş istifadə olunur. Düzgün tətbiq edildikdə xidmət keyfiyyətini və təhlükəsizliyi artırır, lakin məlumat məxfiliyi, yanlış konfigurasiya və xidmət asılılığı kimi risklər də yaradır.

Bulud texnologiyalarının anlayışı və inkişaf xüsusiyyətləri

Bulud texnologiyası istifadəçilərə hesablama resurslarına çevik və tələb əsasında çıxış imkanı verir. NIST əsas xüsusiyyətlər kimi özünəxidmət, elastiklik və ölçülən xidməti göstərir [1]. Bu xüsusiyyətlər buludu ənənəvi hostingdən fərqləndirir.

ISO/IEC 17788 standartına görə bulud hesablama paylaşılan fiziki və virtual resurslardan ibarət elastik modeldir [2]. İstifadəçi xidmətin hansı avadanlıqda işlədiyini bilmədən istifadə edə bilər. Bulud texnologiyalarının inkişafı virtualizasiya, konteyner və avtomatlaşdırma texnologiyaları ilə bağlıdır [3]. Bu yanaşma resurslardan daha səmərəli istifadəyə və çevik idarəetməyə imkan verir. IT şöbələri artıq yalnız avadanlıq deyil, xidmət dizaynı və təhlükəsizlik siyasətinə fokuslanır.

Bulud texnologiyaları müəssisələrə daha sürətli bərpa, global xidmət imkanı və risklərə uyğunlaşma üstünlüyü verir. Buna görə bulud rəqəmsal iqtisadiyyatın əsas infrastruktur komponentlərindən birinə çevrilmişdir.

Xidmət modelləri və yerləşdirmə formaları

Bulud texnologiyalarında əsas xidmət modelləri IaaS, PaaS və SaaS hesab olunur. IaaS istifadəçiyə virtual server, saxlama və şəbəkə resursları təqdim edir, əməliyyat sistemi və tətbiqlərin idarə olunması isə istifadəçinin məsuliyyətində qalır. Bu model çeviklik tələb edən təşkilatlar üçün uygundur.

PaaS proqramçılara tətbiqləri qurmaq və yerləşdirmək üçün hazır mühit təqdim edir. Serverlərin və platforma komponentlərinin idarə olunması provayder tərəfindən həyata keçirilir. Bu

yanaşma innovasiya sürətini artırsa da, platformadan asılılıq riski yarada bilər. SaaS modelində hazır proqram təminatı internet üzərindən təqdim olunur. Elektron poçt, onlayn ofis alətləri və əməkdaşlıq platformaları buna nümunədir. Bu model rahat olsa da, identiklik idarəetməsi, audit qeydləri və müqavilə şərtləri diqqətlə qiymətləndirilməlidir.

Bulud yerləşdirmə modelləri ictimai, özəl, hibrid və çoxbulud formasında qruplaşdırılır [1]. İctimai bulud geniş istifadəçi kütləsinə xidmət edir, özəl bulud isə bir təşkilat üçün xüsusi qurulur. Hibrid bulud lokal və bulud resurslarının birlikdə istifadəsini, çoxbulud isə bir neçə provayderdən istifadəni ifadə edir.

Müasir müəssisələrdə hibrid və çoxbulud yanaşmaları daha çox istifadə olunur. Bunun səbəbi bəzi sistemlərin lokal mühitdə qalması, hüquqi tələblər və bir provayderdən asılılığın risk yaratmasıdır. Buna görə bulud strategiyası texniki imkanlarla yanaşı hüquqi, maliyyə və əməliyyat tələblərinə əsasən formalaşdırılmalıdır.

Bulud arxitekturası, virtualizasiya və konteynerləşmə

Bulud arxitekturası virtual resurslar, şəbəkə və təhlükəsizlik servislərinin birlikdə işləməsinə əsaslanır. Virtualizasiya resurs istifadəsini optimallaşdırır və sistemlərin daha sürətli bərpaasını təmin edir.

Konteyner texnologiyaları və Kubernetes platformaları tətbiqlərin yerləşdirilməsi və idarə olunmasını avtomatlaşdırır. Cloud native yanaşma çevik və davamlı sistemlərin qurulmasına yönəlmişdir [11]. Mikroservis arxitekturası tətbiqləri müstəqil xidmətlərə bölərək çeviklik və miqyaslanma imkanı yaradır, lakin əlavə təhlükəsizlik və monitoring tələb edir.

Bulud arxitekturasında avtomatlaşdırma əsas rol oynayır. İnfrastrukturun kod kimi idarə olunması insan səhvlərini azaldır və təhlükəsizlik nəzarətlərini gücləndirir. AWS Well-Architected Framework və digər çərçivələr təhlükəsiz və dayanıqlı sistemlərin qurulmasını tövsiyə edir [7], [6], [8].

Bulud təhlükəsizliyi və məsuliyyət bölgüsü

Bulud texnologiyalarında təhlükəsizlik əsas məsələlərdəndir. Məsuliyyət provayder və müştəri arasında bölüşdürülür. Provayder infrastrukturunu, müştəri isə məlumatların idarəsi və giriş nəzarətini qoruyur.

Ən böyük risklərdən biri yanlış konfigurasiyadır. Açıq saxlama, zəif identiklik siyasəti və artıq giriş hüquqları məlumat sızmasına səbəb ola bilər. Buna görə ən az imtiyaz prinsipi, çoxfaktorlu autentifikasiya və audit mexanizmləri vacibdir [12]. Məlumatlar saxlanma və ötürülmə zamanı şifrələnməlidir.

Monitoring və hadisə cavabı da mühüm rol oynayır. Audit qeydləri və təhlükə aşkarlama sistemləri risklərin vaxtında müəyyən edilməsinə kömək edir. Cloud Controls Matrix və ENISA çərçivələri bulud risklərinin qiymətləndirilməsi üçün istifadə olunur [9], [10]. Təhlükəsizlik tələbləri dizayn mərhələsindən nəzərə alınmalıdır.

Müəssisələrdə tətbiq strategiyası və migrasiya mərhələləri

Bulud texnologiyalarının tətbiqi planlı strategiya tələb edir. İlk mərhələdə IT mühiti, tətbiqlər, məlumatlar və təhlükəsizlik tələbləri qiymətləndirilməlidir. Əks halda migrasiya əlavə xərclər və təhlükəsizlik riskləri yarada bilər. Microsoft Cloud Adoption Framework bu prosesi strategiya, planlama, hazırlıq, tətbiq və optimallaşdırma mərhələləri ilə izah edir [6].

Migrasiya müxtəlif yanaşmalarla həyata keçirilir. Bəzi sistemlər olduğu kimi buluda köçürülür, digərləri isə cloud native prinsipləri ilə yenidən qurulur. Sürətli köçürmə qısa müddətdə faydalı olsa da, uzunmüddətli problemlər yarada bilər. Yenidən dizayn isə daha çevik və səmərəli nəticə verir. Buluda keçid zamanı tətbiqlərin prioritetləşdirilməsi vacibdir. Pilot layihələr komandaya təcrübə qazandırır və təhlükəsizlik, performans, ehtiyat nüsxə və xərclərin yoxlanılmasına imkan yaradır. Uğurlu migrasiya yalnız texniki yerləşdirmə deyil, istifadəçi məmnuniyyəti və idarəetmə proseslərinin uyğunlaşdırılmasıdır.

Bulud mühitində DevOps və DevSecOps yanaşmaları koordinasiyanı və təhlükəsizliyi gücləndirir. Uğurlu bulud strategiyası biznes məqsədlərinə uyğun qurulmalıdır. Məqsəd xərclərin azaldılmasırsa optimallaşdırma, sürətli inkişafdırsa avtomatlaşdırma, davamlılıqdırsa çoxregionlu arxitektura prioritet seçilməlidir.

Bulud texnologiyalarının iqtisadi təsiri və FinOps yanaşması

Bulud texnologiyalarının əsas üstünlüklərindən biri xərclərin çevik idarə olunmasıdır. Ənənəvi modeldə müəssisələr avadanlığa əvvəlcədən böyük kapital yatırımı etdiyi halda, bulud modelində istifadə olunan xidmətə görə ödəniş edilir. Lakin nəzarətsiz istifadə xərclərin sürətlə artmasına səbəb ola bilər. Avtomatik miqyaslandırma, məlumat saxlanması, şəbəkə istifadəsi və test mühitləri düzgün idarə olunmadıqda büdcə riskləri yaranır.

FinOps yanaşması bulud xərclərinin idarə olunmasında texniki komandalar, maliyyə şöbəsi və rəhbərliyin birlikdə işləməsini nəzərdə tutur. Məqsəd yalnız xərcləri azaltmaq deyil, xərclərin biznes dəyərinə uyğunluğunu təmin etməkdir. Bu baxımdan etikətləmə, büdcə xəbərdarlıqları və hesabat mexanizmləri mühüm rol oynayır. Bulud resurslarının düzgün ölçülməsi də vacibdir. Bəzi tətbiqlər ehtiyacdan böyük resurslardan istifadə edir və ya istifadə olunmayan saxlama obyektləri yüksək xərc yaradır. Buna görə resurslar davamlı izlənməli və biznes tələblərinə uyğun optimallaşdırılmalıdır.

Bulud texnologiyaları kiçik və orta bizneslər üçün də yeni imkanlar açmışdır. Böyük hesablama gücü və ehtiyat infrastrukturunu artıq yüksək kapital tələb etmədən əldə edilə bilər. Bu, innovasiyanı və rəqabəti gücləndirir, lakin səmərəli istifadə üçün texniki bilik və düzgün idarəetmə vacibdir. Buludun iqtisadi təsiri yalnız xərclərlə ölçülür. Sistemlərin daha sürətli hazırlanması, bazara çıxış müddətinin azalması və müştəri təcrübəsinin yaxşılaşması da mühüm dəyər yaradır. Buyya və digər müəlliflər buludu hesablama resurslarının xidmət kimi təqdim olunması modeli ilə əlaqələndirirlər [4].

Buludda verilənlərin idarə olunması və analitika imkanları

Bulud texnologiyaları böyük həcmli məlumatların saxlanması, emalı və təhlilini asanlaşdırır. Obyekt saxlama, paylanmış verilənlər bazaları və analitika xidmətləri müəssisələrə avadanlıq idarə etmədən məlumat üzərində işləməyə imkan verir.

Məlumat anbarı strukturlaşdırılmış məlumatları, data lake isə müxtəlif tip məlumatları saxlamaq üçün istifadə olunur. Bu yanaşmalar birlikdə analitika və süni intellekt tətbiqlərini dəstəkləyir. Lakin əsas məsələ məlumatın keyfiyyəti və düzgün idarə olunmasıdır. Bulud analitikası real vaxt qərarverməsini gücləndirir. Elektron ticarət, bank və sənaye sektorlarında istifadəçi davranışı, əməliyyat anomaliyaları və avadanlıq riskləri daha tez təhlil edilə bilər. Bu da buludu yalnız saxlama deyil, qərarvermə platformasına çevirir.

Məlumatların buludda idarə olunması zamanı məxfilik və uyğunluq vacibdir. Həssas məlumatlar şifrələnməli, girişlər məhdudlaşdırılmalı və audit izlənilirliyi təmin edilməlidir. Buludun əsas üstünlüklərindən biri çevik genişlənmədir. Məlumat artdıqca saxlama resursları asanlıqla artırıla bilər. Lakin düzgün arxiv siyasəti və məlumat idarəetməsi həm xərcləri, həm də təhlükəsizlik risklərini azaltmaq üçün vacibdir.

Risklər, uyğunluq və xidmət keyfiyyəti məsələləri

Bulud texnologiyaları geniş imkanlar yaratsa da, risklərin düzgün idarə olunmasını tələb edir. Əsas risklərdən biri vendor lock-in, yəni bir provayderdən asılılıqdır. Açıq standartlar, konteynerləşmə və məlumat ixrac planları bu riski azaltmağa kömək edir.

Uyğunluq məsələləri xüsusilə bank, səhiyyə və dövlət sektorunda vacibdir. Məlumatların saxlanması, audit və giriş nəzarətləri ciddi qaydalarla tənzimlənir. Provayderin sertifikatları kifayət deyil, müəssisə öz təhlükəsizlik proseslərini ayrıca idarə etməlidir. Xidmət səviyyəsi razılaşmaları da diqqətlə qiymətləndirilməlidir. Yüksək əlçatanlıq vədi olsa belə, zəif arxitektura biznes dayanmasına səbəb ola bilər. Buna görə yalnız provayder deyil, sistem dizaynı da vacibdir.

Bulud mühitində insan faktoru böyük risk yaradır. Səhv giriş hüquqları, zəif parollar və təcrübəsiz idarəetmə ciddi problemlərə səbəb ola bilər. Bu riskləri azaltmaq üçün təlim, siyasət əsaslı idarəetmə və avtomatik nəzarət mexanizmləri tətbiq edilməlidir. Risklərin azaldılması üçün müəssisə əvvəlcədən bulud idarəetmə modeli qurmalıdır. Buraya resurs idarəetməsi, təhlükəsizlik monitorinqi, ehtiyat nüsxə siyasəti və xərclərin nəzarəti daxildir. NIST Cloud Computing Standards Roadmap standartlaşdırmanın təhlükəsizlik və sabitlik baxımından vacibliyini vurğulayır [5].

Bulud texnologiyalarının Azərbaycanca və regional müəssisələrdə perspektivləri

Azərbaycanda və region ölkələrində rəqəmsallaşma bulud texnologiyalarına marağı artırır. Elektron dövlət xidmətləri, rəqəmsal bankçılıq, distant təhsil və onlayn səhiyyə sistemləri bulud infrastrukturundan geniş istifadə edir. Bulud texnologiyaları xidmətlərin əlçatanlığını, təhlükəsizliyini və çevik miqyaslanmasını təmin edir.

Buludun əsas üstünlüklərindən biri ilkin sərmayə yükünü azaltmasıdır. Kiçik və orta biznes öz məlumat mərkəzini qurmadan müasir proqram və xidmətlərdən istifadə edə bilər. Lakin internet sabitliyi, məlumatların saxlanma yeri və mütəxəssis çatışmazlığı kimi problemlər nəzərə alınmalıdır. Dövlət və kritik infrastruktur sahələrində daha çox özəl və hibrid bulud yanaşmaları tətbiq olunur. Bu sahələrdə məlumatların ölkə daxilində saxlanması və təhlükəsizlik auditləri vacibdir. Təhsil müəssisələrində isə bulud texnologiyaları virtual laboratoriyalar və onlayn əməkdaşlıq mühiti yaradaraq praktiki tədrisi gücləndirir.

Regional inkişaf üçün yalnız bulud xidmətlərindən istifadə kifayət deyil. Bulud təhlükəsizliyi, DevOps, məlumat idarəetməsi və uyğunluq üzrə yerli mütəxəssis hazırlığı da artırılmalıdır. Bu yanaşma innovasiya və xidmət keyfiyyətinin yüksəlməsinə kömək edir.

Gələcək inkişaf istiqamətləri

Bulud texnologiyalarının inkişafında əsas istiqamətlərdən biri edge computing-dir. Bu yanaşma hesablama resurslarını istifadəçiyə yaxınlaşdıraraq gecikməni azaldır və real vaxt emalını sürətləndirir. Digər istiqamət serverless arxitektura. Burada proqramçı server idarə etmir, kod yalnız hadisə baş verdikdə işləyir. Bu model çevik və avtomatik miqyaslanma biləndir, lakin provayder asılılığı və monitoring çətinlikləri yarada bilər.

Süni intellekt və buludun birləşməsi də mühüm inkişaf istiqamətidir. Bulud provayderləri maşın öyrənməsi və generativ AI xidmətlərini daha əlçatan edir. Bununla yanaşı, məlumat məxfiliyi, etik istifadə və xərclərin idarəsi vacib olaraq qalır. Davamlılıq və enerji səmərəliliyi də ön plana çıxır. Resursların optimallaşdırılması və lazımsız sistemlərin söndürülməsi həm xərcləri, həm də enerji sərfiyyatını azaldır [8].

Gələcəkdə bulud texnologiyaları daha avtomatlaşdırılmış və ağıllı idarəetmə modelinə keçəcək. Süni intellekt dəstəkləyən sistemlər təhlükəsizlik risklərini və nasazlıqları daha tez müəyyən edə biləcək, lakin strateji qərarlarda insan rolu qalacaq.

Nəticə

Aparılan təhlil göstərir ki, bulud texnologiyaları müasir informasiya texnologiyalarının əsas istiqamətlərindən biridir. Bulud modeli müəssisələrə resurslardan tələb əsasında istifadə etməyə, tətbiqləri sürətlə yerləşdirməyə və xidmət imkanlarını genişləndirməyə şərait yaradır.

Bununla yanaşı, yanlış konfigurasiya, məlumat məxfiliyi, uyğunluq tələbləri, xidmət asılılığı və nəzarətsiz xərclər kimi risklər də mövcuddur. Bu səbəbdən bulud strategiyası təhlükəsizlik, maliyyə idarəetməsi, düzgün arxitektura və təşkilati dəyişikliklər nəzərə alınaraq hazırlanmalıdır.

Bulud texnologiyalarından səmərəli istifadə yalnız texniki migrasiya deyil, həm də iş yüklərinin təhlili, xidmət modelinin seçilməsi, təhlükəsizlik nəzarətlərinin tətbiqi və davamlı optimallaşdırma tələb edir. Nəticə olaraq, düzgün planlaşdırılmış bulud strategiyası müəssisələrə çeviklik, etibarlılıq, təhlükəsizlik və innovasiya üstünlüyü qazandıra bilər.

Ədəbiyyat

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Special Publication 800-145. <https://doi.org/10.6028/NIST.SP.800-145>
2. ISO/IEC. (2014). ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary. International Organization for Standardization.
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58. <https://doi.org/10.1145/1721654.1721672>

4. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599-616. <https://doi.org/10.1016/j.future.2008.12.001>
5. Hogan, M., Liu, F., Sokol, A., & Tong, J. (2013). NIST Cloud Computing Standards Roadmap, Special Publication 500-291, Version 2. National Institute of Standards and Technology.
6. Microsoft. (2025). Microsoft Cloud Adoption Framework for Azure. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/>
7. Amazon Web Services. (2024). AWS Well-Architected Framework. Amazon Web Services Documentation. <https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html>
8. Google Cloud. (2026). Google Cloud Well-Architected Framework. Google Cloud Architecture Center. <https://docs.cloud.google.com/architecture/framework>
9. Cloud Security Alliance. (2026). Cloud Controls Matrix and CAIQ v4.1. Cloud Security Alliance. <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1>
10. European Union Agency for Cybersecurity. (2009). Cloud Computing: Benefits, risks and recommendations for information security. ENISA.
11. Cloud Native Computing Foundation. (2024). Cloud Native Definition v1.1. CNCF Technical Oversight Committee. <https://github.com/cncf/toc/blob/main/DEFINITION.md>
12. Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144. <https://doi.org/10.6028/NIST.SP.800-144>