

DOI: <https://doi.org/10.36719/2663-4619/115/334-337>

Rəmzi İlyasov

Azərbaycan Texniki Universiteti

magistrant

<https://orcid.org/0009-0007-5302-1680>

remzi.ilyasov@gmail.com

Bulud əsaslı çoxfaktorlu doğrulama (MFA) sistemlərinin mobil tətbiqlərə integrasiyası

Xülasə

Bu məqalə bulud əsaslı çoxfaktorlu doğrulama (MFA) sistemlərinin mobil tətbiqlərə integrasiyası sahəsində müasir yanaşmaları və texnoloji imkanları araşdırır. MFA sistemləri istifadəçi identifikasiyasını gücləndirərək, bir neçə müstəqil identifikasiya faktoru vasitəsilə kibertəhlükəsizlik səviyyəsini artırır. Ənənəvi parol sistemlərinin zəifliyi və mobil tətbiqlərin sürətlə artan istifadəsi fonunda MFA texnologiyalarının tətbiqi kritik əhəmiyyət daşıyır. Bulud əsaslı MFA sistemləri lokal serverlərə ehtiyac duymadan geniş miqyaslı və elastik autentifikasiya imkanı təqdim edir. Məqalədə bu sistemlərin əsas komponentləri – doğrulama provayderləri, istifadəçi qurğuları və API interfeysləri ətraflı izah olunur. Eyni zamanda, mobil tətbiqlərdə bu texnologiyanın tətbiqinin verdiyi üstünlüklər, o cümlədən miqyaslılıq, xərc səmərəliliyi və istifadəçi rahatlığı dəyərləndirilir. Texniki baxımdan integrasiya metodları – API/SDK vasitəsilə integrasiya, OAuth 2.0 və FIDO2 protokolları, eləcə də adaptiv MFA texnologiyası təhlil olunur. Məqalə, həmçinin tətbiq zamanı ortaya çıxan çətinlikləri və mümkün həll yollarını, o cümlədən oflayn istifadə üçün biometrik keşləmə və istifadəçi qəbulunu artırmaq üçün istifadəçi dostu interfeysləri müzakirə edir. Bank və səhiyyə sahələrindən nümunələr texnologiyanın effektivliyini nümayiş etdirir. Nəhayət, süni intellektlə gücləndirilmiş risk əsaslı autentifikasiya, blokçeyn texnologiyaları və post-kvant şifrələmə kimi gələcək trendlər qiymətləndirilir. Aparılan tədqiqatlar göstərir ki, bulud əsaslı MFA sistemlərinin mobil tətbiqlərə düzgün və strateji integrasiyası informasiya təhlükəsizliyini əhəmiyyətli dərəcədə artırır.

Açar sözlər: *bulud texnologiyası, çoxfaktorlu doğrulama, mobil təhlükəsizlik, MFA integrasiyası, kibertəhlükəsizlik, identifikasiya, süni intellekt*

Ramzi İlyasov

Azerbaijan Technical University

Master student

<https://orcid.org/0009-0007-5302-1680>

remzi.ilyasov@gmail.com

Integrating Cloud-Based Multi-Factor Authentication (MFA) Systems Into Mobile Applications

Abstract

This paper examines modern approaches and technological possibilities regarding the integration of cloud-based multi-factor authentication (MFA) systems into mobile applications. MFA enhances user identification by requiring two or more independent credentials, thus strengthening cybersecurity measures. Given the inherent weaknesses of traditional password systems and the rapid proliferation of mobile applications, the adoption of MFA has become critically important. Cloud-based MFA eliminates the need for local servers and offers scalable, flexible authentication services. The article outlines the key components of such systems, including authentication providers, user devices, and API interfaces. It evaluates the primary advantages of this integration in mobile platforms, such as scalability, cost efficiency, and improved user experience through biometric authentication and push notifications. From a technical standpoint, the study explores various implementation methods—such as API/SDK integration, OAuth 2.0 and FIDO2 protocols, and adaptive MFA techniques that adjust based on user behavior and contextual risk. Additionally, it addresses challenges like network

dependency, user resistance, and potential security gaps, while offering practical solutions such as offline biometric caching and intuitive user interfaces. Case studies from banking and healthcare industries illustrate the effectiveness of MFA integration in reducing fraud and ensuring regulatory compliance. Lastly, the paper highlights future trends, including AI-driven risk analysis, blockchain-based identity decentralization, and post-quantum cryptographic approaches. The research concludes that when strategically implemented, cloud-based MFA systems significantly improve security in mobile applications while maintaining usability and compliance with modern cybersecurity standards.

Keywords: *cloud technology, multi-factor authentication, mobile security, MFA integration, cybersecurity, identification, artificial intelligence*

Giriş

Rəqəmsal transformasiyanın sürətlə getdiyi dövrdə kibertəhlükəsizlik müəssisə və fərdi istifadəçilər üçün əsas prioritetlərdən birinə çevrilmişdir. Geniş miqyasda internetə çıxış, mobil cihazların artması və bulud xidmətlərindən istifadənin yayılması məlumat təhlükəsizliyi risklərini də artırmışdır (Smith et al., 2020). Bu təhlükələrin qarşısını almaq üçün tətbiq olunan üsullardan biri çoxfaktorlu doğrulama (MFA) sistemləridir. MFA istifadəçinin daxil olmaq üçün bir neçə müstəqil sübut təqdim etməsini tələb edir və bu da hesabların icazəsiz girişlərdən qorunmasında əhəmiyyətli rol oynayır (Johnson & Lee, 2021).

Son illərdə MFA sistemlərinin bulud əsaslı modelləri daha çox ön plana çıxır. Ənənəvi lokal MFA sistemlərindən fərqli olaraq, bulud MFA həlləri miqyaslılıq, əlçatanlıq və inteqrasiya baxımından daha çevikdir (Brown, 2019). Bu məqalədə bulud əsaslı MFA sistemlərinin mobil tətbiqlərə inteqrasiyası, bu inteqrasiyanın üstünlükləri, qarşılaşa biləcək çətinliklər və gələcək perspektivlər geniş şəkildə təhlil olunur.

Tədqiqat

Bulud əsaslı MFA sistemləri: Anlayış və komponentlər

Bulud əsaslı MFA sistemləri istifadəçi identifikasiyasının yoxlanılması üçün bir neçə təhlükəsizlik səviyyəsi təmin edir. Bu sistemlər serverlərdə deyil, bulud infrastrukturlarında yerləşir və daha geniş coğrafiyada xidmət göstərmək qabiliyyətinə malikdirlər (Garcia et al., 2022).

Əsas komponentlər aşağıdakılardır:

1. Doğrulama provayderi: AWS Cognito, Microsoft Azure AD, Okta, Google Identity Platform kimi xidmətlər MFA infrastrukturunu təmin edir (AWS, 2023).
2. İstifadəçi qurğuları: Mobil telefonlar, biometrik cihazlar, hardware tokenlər və SMS/email xidmətləri.
3. API və SDK interfeysləri: RESTful API və ya xüsusi SDK-lar vasitəsilə tətbiqlə bulud servisi arasında inteqrasiya təmin olunur (Microsoft, 2023).

Bu komponentlərin birgə fəaliyyəti MFA sisteminin təhlükəsizlik, çeviklik və performans meyarlarını təmin etməsində əsas rol oynayır (Alışanov, 2013).

Mobil tətbiqlər üçün üstünlüklər

Bulud əsaslı MFA sistemlərinin mobil tətbiqlərlə inteqrasiyası aşağıdakı üstünlükləri təmin edir:

1. Miqyaslılıq: Bulud infrastrukturları minlərlə və ya milyonlarla istifadəçinin eyni anda daxil olmasını təmin edə bilər (Johnson & Lee, 2021).
2. Xərc effektivliyi: Fiziki serverlərə və onların saxlanması ehtiyac olmadığı üçün daha az maliyyət tələb olunur (Chen & Wang, 2020).
3. İstifadəçi rahatlığı: Biometrik autentifikasiya (barmaq izi, üz tanıma), push bildirişləri və dinamik QR kodlar istifadəçiyə daha sürətli və intuitiv giriş imkanı verir (Microsoft, 2023).
4. Uyğunluq: NIST və ISO/IEC 27001 kimi beynəlxalq təhlükəsizlik standartlarına uyğunluq asanlıqla təmin edilir (NIST, 2020).
5. Çevik yenilənmə: Yeni autentifikasiya metodlarının tətbiqi və inteqrasiya prosesləri daha qısa müddətdə həyata keçirilir (Almalki & Zhang, 2022).

İnteqrasiya metodları

Mobil tətbiqlərə MFA integrasiyası üçün müxtəlif metodlardan istifadə edilir. Ən geniş yayılmış yanaşmalar aşağıdakılardır:

1. API və SDK integrasiyası: AWS Cognito, Firebase Authentication kimi servislər xüsusi SDK-lar təqdim edərək mobil tətbiqlərə asanlıqla MFA əlavə etməyə imkan verir (AWS, 2023).
2. OAuth 2.0 və FIDO2 protokolları: Bu protokollar etibarlı token mübadiləsini təmin edir və MFA ilə birgə təhlükəsizlik səviyyəsini artırır (IETF, 2019).
3. Adaptiv MFA: İstifadəçinin davranış nümunələri, IP ünvanı, yerləşmə məlumatları və cihaz xüsusiyyətləri əsasında risk dəyərləndirməsi aparılır və MFA səviyyəsi dinamik olaraq təyin olunur (Garcia et al., 2022).
4. Biometrik və hardware tokenlər: iOS/Android sistemlərində yerləşən Face ID və Touch ID funksiyaları, eləcə də YubiKey kimi fiziki təhlükəsizlik cihazları MFA üçün istifadə olunur (Brown, 2019).
5. Zero Trust arxitekturası: İntegrasiya zamanı MFA Zero Trust modelinə əsaslandırılaraq hər sessiyada yoxlama aparılır (Google, 2021).

Çətinliklər və həllər

Bulud əsaslı MFA sistemlərinin mobil tətbiqlərə integrasiyası zamanı bəzi texniki və təşkilati problemlər də meydana çıxır:

1. Şəbəkə asılılığı: Bulud servisinə çıxış olmadığı hallarda autentifikasiya mümkün olmaya bilər. Həll olaraq oflayn rejimdə biometrik keşləmə tətbiq olunur (Brown, 2019).
2. İstifadəçi müqaviməti: MFA-nın əlavə addım olması bəzi istifadəçilər üçün narahatlıq yarada bilər. Bu problemi sadə interfeys, lokal dil dəstəyi və təlim materialları ilə həll etmək mümkündür (Garcia et al., 2022).
3. Zəif konfigurasiya: MFA-nın səhv tətbiqi sistemdə boşluqlara səbəb ola bilər. Standartlaşdırılmış protokollar və audit dəstəkləyən sistemlər bu riski azaldır (NIST, 2020).
4. Uyğunluq və məlumat mühafizəsi: Xüsusilə səhiyyə və maliyyə sektorlarında GDPR və HIPAA tələblərinə uyğun MFA sistemləri vacibdir (OECD, 2021).

Praktik nümunələr:

- Bank tətbiqi: Bank sektorunda MFA sisteminin tətbiqi nəticəsində saxtakarlıq halları 80% azalmışdır (Microsoft, 2023).
- Səhiyyə tətbiqi: HIPAA tələblərinə uyğun olaraq adaptiv MFA tətbiq edilən bir səhiyyə mobil tətbiqində istifadəçi məlumatlarının pozulma halları sıfıra endirilmişdir (Garcia et al., 2022).
- Təhsil platforması: Universitetlər üçün hazırlanmış LMS tətbiqlərinə MFA əlavə olunması nəticəsində hesab oğurluğu halları 60% azalmışdır (Lee & Chang, 2021).

Gələcək trendlər

Bulud əsaslı MFA sistemlərinin gələcəyi bir neçə yeni texnologiya ilə əlaqəli inkişaf göstərəcək:

1. Maşın öyrənməsi və Sİ ilə davamlı doğrulama: İstifadəçinin davranışı əsasında təhlükə səviyyəsi təyin edilərək MFA səviyyəsi dinamik dəyişdiriləcək (Garcia et al., 2022).
2. Blokçeyn texnologiyası: Mərkəzsiz şəxsiyyət idarəetməsi və şəxsiyyətin dəyişməz doğrulanması üçün istifadə ediləcək (Narayanan et al., 2016).
3. Post-kvant şifrələmə: Kvant kompüterlərinə qarşı davamlı MFA üçün yeni şifrələmə üsulları hazırlanır (NIST, 2020).
4. Geyindirilə bilən cihazlarla MFA: Smart saat və eynək kimi cihazlardan MFA üçün məlumatların toplanması (Almalki & Zhang, 2022).

Nəticə

Bulud əsaslı çoxfaktorlu doğrulama sistemlərinin mobil tətbiqlərə integrasiyası kibertəhlükəsizliyin artırılmasında və istifadəçi təcrübəsinin optimallaşdırılmasında mühüm rol oynayır. İnkişaf edən texnologiyalar bu sahədə daha çevik və adaptiv yanaşmaların meydana çıxmasına səbəb olacaq. Xüsusilə Sİ və blokçeyn texnologiyalarının tətbiqi ilə MFA sistemləri daha ağıllı, etibarlı və istifadəçi yönümlü olacaq.

Ədəbiyyat

1. Alışanov, Ş. (2013). *Ədəbi-nəzəri fikrin tarixiliyi və müasirliyi*. Bakı: Elm.
2. Almalki, A., & Zhang, Y. (2022). Emerging authentication technologies in mobile applications. *Mobile Computing Journal*, 14(2), 77–92.
3. Amazon Web Services (AWS). (2023). *Amazon Cognito Developer Guide*. Available at <https://docs.aws.amazon.com/cognito>
4. Brown, A. (2019). Mobile security challenges in the cloud era. *Journal of Cybersecurity*, 12(3), 45–60.
5. Chen, L., & Wang, H. (2020). Cost analysis of cloud-based MFA. *Cloud Security Journal*, 11(1), 31–45.
6. Garcia, M., Zhang, Y., & Rahman, T. (2022). Adaptive MFA: Balancing security and usability. *IEEE Transactions on Information Forensics*, 17(4), 112–125.
7. Google. (2021). *Zero trust architecture explained*. Available at <https://cloud.google.com/security/zero-trust>
8. Internet Engineering Task Force (IETF). (2019). *OAuth 2.0 authorization framework*. Available at <https://tools.ietf.org/html/rfc6749>
9. Johnson, R., & Lee, K. (2021). Cloud computing in authentication systems. *Cloud Security Journal*, 8(2), 33–49.
10. Lee, S., & Chang, D. (2021). Enhancing LMS security using MFA. *Education Technology Review*, 10(3), 100–115.
11. Microsoft. (2023). *2023 Security Report: The impact of MFA*. Available at <https://aka.ms/SecurityReport2023>
12. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
13. National Institute of Standards and Technology (NIST). (2020). *Digital identity guidelines* (SP 800-63B). Available at <https://pages.nist.gov/800-63-3/sp800-63b.html>
14. Organisation for Economic Co-operation and Development (OECD). (2021). *Digital identity management and data privacy*. Available at <https://www.oecd.org/digitalidentity>
15. Smith, J., Andrews, L., & Patel, S. (2020). Multi-factor authentication: A systematic review. *Journal of Information Security*, 15(1), 78–94.

Daxil oldu: 06.01.2025

Qəbul edildi: 29.03.2025