Orxan Vaqif oğlu KAZIMOV
Qərbi Kaspi Universiteti, Idarəetmədə İnformasiya sistemləri üzrə magistrant
E-mail: orkhankazimli@gmail.com
ORCID ID: 0009-0007-4328-2430

RƏQƏMSAL TƏHSİLDƏ ETİMADIN QURULMASI: MOBİL ÖYRƏNMƏ PLATFORMALARINDA MFA-NIN TEXNİKİ ARXİTEKTURASI VƏ STRATEJİ ÜSTÜNLÜKLƏRİ

Xülasə

Mobil texnologiyaların təhsil sektoruna sürətli inteqrasiyası öyrənmə prosesini zaman və məkan məhdudiyyətindən azad etsə də, eyni zamanda ciddi kibertəhlükəsizlik boşluqları yaratmışdır. Bu məqalədə mobil təhsil (m-learning) ekosistemlərində istifadəçi məlumatlarının qorunması və akademik dürüstlüyün təmin edilməsi üçün Çoxfaktorlu Autentifikasiyanın (MFA) tətbiqi mexanizmləri tədqiq olunur. Tədqiqat çərçivəsində MFA-nın bulud əsaslı Təhsil İdarəetmə Sistemlərinə (LMS) inteqrasiya arxitekturası, biometrik identifikasiya metodlarının texniki üstünlükləri və bu texnologiyanın tələbə təcrübəsinə (UX) təsiri təhlil edilir. Məqalədə vurğulanır ki, MFA yalnız kiberhücumlardan qorunma vasitəsi deyil, həm də rəqəmsal transformasiya dövründə təhsil müəssisələrinin institusional nüfuzunu qoruyan strateji bir elementdir. Tədqiqatın sonunda mobil təhsil platformaları üçün adaptiv və istifadəçi dostu autentifikasiya modelləri təklif olunur.

Açar sözlər: mobil təhsil, MFA, kibertəhlükəsizlik, rəqəmsal transformasiya, biometrik autentifikasiya.

UOT: 004.738.5:004.056.5:37.018.43
JEL: O33, I21
DOI: https://doi.org/10.54414/FOFB1380

Giriş

1. Mobil təhsilin (m-Learning) təkamülü: texnoloji və pedaqoji paradiqma dəyişikliyi. XXI əsrin başlanğıcı informasiya texnologiyalarının təhsil sektorunda tətbiqi baxımından inqilabi bir dövr kimi xarakterizə olunur. İnternet texnologiyalarının və fərdi hesablama sistemlərinin inkişafı əvvəlcə elektron təhsili (e-learning) gündəmə gətirsə də, son onillikdə mobil rabitə şəbəkələrinin (4G/5G) və smart cihazların kütləviləşməsi bizi Mobil Təhsil (m-learning) erasına daşımışdır. Bu keçid sadəcə cihazların ölçüsünün kiçilməsi deyil, təhsilin fəlsəfəsində baş verən fundamental paradiqma dəyişikliyidir. Ənənəvi təhsil modelində bilik müəyyən bir məkana (sinif otağı) və zamana (dərs saatı) indeksləndiyi halda, mobil təhsil bu sərhədləri darmadağın edərək "fasiləsiz öyrənmə" (lifelong learning) modelini əlçatan etmişdir.

Statistik göstəricilər bu sürətli keçidi aydın şəkildə əks etdirir. UNESCO-nun hesabatlarına görə, qlobal miqyasda ali təhsil alan tələbələrin 80%-dən çoxu gündəlik akademik fəaliyyətlərində — mühazirələri dinləməkdən tutmuş, tədqiqat aparmağa qədər — mobil cihazlardan istifadə edir. Mobil platformalar tələbələrə interaktiv LMS (Learning Management Systems) interfeysləri, bulud əsaslı kitabxanalar və real-vaxt rejimində əməkdaşlıq alətləri təklif edir. Lakin bu texnoloji lütfün arxa planında, rəqəmsal dünyanın ən kritik problemi — təhlükəsizlik boşluğu dayanır. Təhsilin demokratikləşməsi və əlçatanlığın maksimallaşdırılması, təəssüf ki, kibertəhlükəsizlik standartlarının eyni sürətlə inkişaf etmədiyi bir mühitdə baş vermişdir [7].

Problemin qoyuluşu: rəqəmsal sərhədlərin zəifliyi və artan təhdid landşaftı. Mobil cihazların təhsil ekosisteminə bu qədər dərindən nüfuz etməsi, kiber-cinayətkarlar üçün geniş bir "hücum səthi" (attack surface)

yaratmışdır. Əvvəllər universitet şəbəkələri daxili firewall-lar və mərkəzləşdirilmiş sistemlərlə qorunurdusa, indi hər bir tələbənin şəxsi smartfonu təhsil müəssisəsinin şəbəkəsinə açılan bir qapıdır. Bu cihazların çoxu ictimai Wi-Fi şəbəkələrindən istifadə edir, zəif kiber-gigiyenaya malikdir və çox vaxt təhlükəsizlik yeniləmələrindən məhrumdur.

Ənənəvi autentifikasiya üsulları, xüsusilə də yalnız statik şifrələrə əsaslanan sistemlər, müasir hücum metodları qarşısında aciz qalmışdır. Microsoft-un kibertəhlükəsizlik hesabatlarına görə, yalnız şifrə ilə qorunan hesabların ələ keçirilmə ehtimalı, MFA ilə qorunan hesablardan 99% daha çoxdur. Təhsil sektorunda baş verən məlumat sızmaları təkcə fərdi məlumatların (ad, ünvan, maliyyə məlumatları) oğurlanması ilə bitmir; bu, həm də akademik dürüstlüyün manipulyasiyasına — qiymətlərin dəyişdirilməsi, imtahan suallarının sızdırılması və saxta akademik profillərin yaradılmasına gətirib çıxarır. Bu vəziyyət təhsil müəssisələrinin institusional nüfuzuna və diplomların beynəlxalq legitimliyinə birbaşa təhlükə yaradır. Şifrələrin asanlıqla qırılması, *phishing* (fırıldaqçılıq) və *credential stuffing* kimi texnikaların geniş yayılması rəqəmsal təhsilin gələcəyini sual altına qoyur.

Məqalənin məqsədi: təhlükəsizlikdə yeni standartın müəyyənləşdirilməsi. Bu tədqiqatın əsas məqsədi, Çoxfaktorlu Autentifikasiyanın (MFA) mobil təhsildə tətbiqinin sadəcə bir texniki əlavə və ya istifadəçi üçün "əlavə addım" deyil, rəqəmsal təhsil arxitekturasının təməl daşı olduğunu elmi və praktiki tərəfdən əsaslandırmaqdır. MFA, istifadəçinin şəxsiyyətini təsdiqləmək üçün müstəqil faktorların (bildiyiniz bir şey, sahib olduğunuz bir şey və olduğunuz bir şey) kombinasiyasını tələb edərək, təhlükəsizlik səviyyəsini keyfiyyətcə yeni mərhələyə qaldırır. Məqalə çərçivəsində MFA-nın mobil təhsil mühitindəki rolu üç kritik müstəvidə dərindən təhlil ediləcəkdir:

1. Texniki analiz: MFA-nın müasir LMS platformalarına inteqrasiya imkanları və bulud əsaslı arxitekturalarda işləmə mexanizmləri.
2. Təhlükəsizlik effektivliyi: Spesifik kiber-təhdidlərin neytrallaşdırılmasında biometrik və dinamik autentifikasiya metodlarının rolu.
3. İstifadəçi psixologiyası və UX: təhlükəsizlik tədbirləri ilə tələbə məmnuniyyəti arasındakı balansın qorunması və rəqəmsal transformasiyanın etik aspektləri.

Biz iddia edirik ki, MFA-nın strateji tətbiqi mobil təhsildə yalnız kiber-insidentlərin sayını azaltmır, həm də tələbələr, müəllimlər və təhsil inzibatçıları arasında "rəqəmsal etimad" (digital trust) şəbəkəsini bərpa edir. Bu etimad isə müasir təhsilin gələcək dayanıqlığının və rəqəmsal suverenliyinin ən vacib komponentidir.

2. Mobil təhsildə təhlükəsizlik landşaftı: təhdidlər və qorunma mexanizmləri. Mobil təhsil platformalarının (m-Learning) genişlənməsi təkcə təhsilin əlçatanlığını deyil, həm də kiber-hücumlar üçün hədəf kütləsini eksponensial şəkildə artırmışdır. Bu bölmədə biz mobil mühitdəki təhlükəsizlik boşluqlarını "insan faktoru", "hücum metodologiyası" və "texnoloji baryer" prizmasından ətraflı təhlil edəcəyik.

2.1. Zəif şifrə problemi: kibertəhlükəsizliyin psixoloji və texniki "Aşil dabanı". Mobil təhsil platformalarında autentifikasiya məsələsi kiber-müdafiənin ən mühüm səngərinə çevrilmişdir. Lakin statistikalar göstərir ki, rəqəmsal dünyanın "yerli sakinləri" (digital natives) hesab olunan müasir tələbə kontingenti, paradoksal olaraq, kiber-gigiyena qaydalarına qarşı ən laqeyd qruplardan biridir.

- Şifrə yorğunluğu (Password Fatigue): Tələbələrin akademik həyatı boyunca onlarla platformada (LMS, elektron kitabxana, portal, e-poçt və s.) qeydiyyatdan keçməsi onları "şifrə yorğunluğuna" sövq edir. Nəticədə, tələbələrin təxminən 70-75%-i asan xatırlanan, lakin kiber-müdafiə baxımından sıfır effektivliyə malik olan "123456", "qwerty", yaxud öz doğum tarixləri və universitet adlarından ibarət şifrələrə üstünlük verirlər [3].
- Mobil klaviaturanın məhdudiyyətləri: Mobil cihazlarda mürəkkəb simvolların (!, @, #, $, &) daxil edilməsi fiziki klaviatura ilə müqayisədə daha çox vaxt və diqqət tələb edir. Bu erqonomik çətinlik istifadəçiləri şüuraltı olaraq mürəkkəb şifrələrdən qaçmağa və sadə, yalnız hərf-rəqəm kombinasiyalarına yönəldir [6].

- Zəncirvari təhlükə: Bir tələbənin sosial media hesabında istifadə etdiyi zəif şifrə, onun universitet portalındakı akademik məlumatlarının da açarı olur. Kiber-cinayətkarlar üçün bir "giriş nöqtəsi" bütün təhsil müəssisəsinin mərkəzləşdirilmiş məlumat bazasına sızmaq üçün ilkin tramplin rolunu oynayır.

2.2. Kiberhücum növləri: təhsil sektorunun spesifik təhdidləri. Mobil mühitdə tələbə və müəllim heyəti hər an müxtəlif, getdikcə mürəkkəbləşən hücum metodologiyaları ilə üz-üzədir.

a) Genişlənmiş Phishing (Fırıldaqçılıq) taktikaları: Mobil cihazlarda e-poçt interfeysləri ünvan sətrini (URL) qısaldır və ya tam gizlədir. Bu, tələbələrin saxta bir LMS giriş səhifəsini orijinalından fərqləndirməsini qeyri-mümkün edir. Müasir phishing hücumları artıq sadə e-poçtlarla məhdudlaşmır; Smishing (SMS vasitəsilə phishing) və Vishing (səsli zənglər) vasitəsilə tələbələrə "Təcili təqaüd sənədi təsdiqi" və ya "İmtahan nəticələrində xəta" kimi manipulyativ mesajlar göndərilir. Linkə keçid edən tələbə öz identifikasiya məlumatlarını öz əli ilə hücumçuya təslim edir [7].

b) Credential Stuffing və avtomatlaşdırılmış bot hücumları: Bu metod kibercinayətkarların qara bazarda (Dark Web) satılan sızdırılmış məlumat bazalarından istifadə etməsinə əsaslanır. Bir universitet portalına saniyədə minlərlə giriş cəhdi edən botlar, tələbələrin eyni şifrəni bir neçə yerdə istifadə etmə vərdişindən yararlanırlar. Mobil cihazların daimi onlayn statusu bu cür hücumların fon rejimində, istifadəçi hiss etmədən həyata keçirilməsinə şərait yaradır [7].

c) Man-in-the-Middle (MitM) və ictimai Wi-Fi təhlükəsi: Mobil təhsilin mahiyyəti "hər yerdə öyrənmək"dir. Bu isə tələbələrin kafelərdə, nəqliyyatda və ya kitabxanalarda olan qorunmayan ictimai Wi-Fi şəbəkələrindən istifadə etməsi deməkdir. Bu şəbəkələr üzərindən ötürülən şifrələr və sessiya tokenləri xüsusi proqram təminatları vasitəsilə asanlıqla ələ keçirilə bilir [7].

2.3. MFA-nın müdafiə mexanizmi: çoxqatlı "keçilməz divar" strategiyası. Bu kompleks təhdidlərə qarşı Çoxfaktorlu Autentifikasiya (MFA) müasir mobil təhsilin ən etibarlı müdafiə sədri — "rəqəmsal qalxanı" kimi çıxış edir. MFA-nın fəlsəfəsi təhlükəsizliyi bir nöqtədən (şifrə) asılılıqdan xilas edib, onu üç müstəqil sütun üzərində qurmaqdır:

1. Bilmə faktoru (Something you know): Parol və ya PİN-kod.
2. Sahib olma faktoru (Something you have): Smartfon, hardware token və ya birdəfəlik kod generatoru.
3. Mövcudluq faktoru (Something you are): Biometrik datalar (barmaq izi, üz cizgiləri, səs).

MFA necə "keçilməz divar" yaradır? Təsəvvür edək ki, bir kiber-hücumçu phishing vasitəsilə tələbənin şifrəsini ələ keçirib. Ənənəvi sistemlərdə bu, hücumun qələbəsi deməkdir. Lakin MFA tətbiq olunmuş sistemdə hücumçu "birinci divarı" keçsə də, dərhal ikinci səddə toqquşur. Sistem tələbənin mobil telefonuna Push-bildiriş göndərir və ya biometrik təsdiq tələb edir. Hücumçu fiziki olaraq tələbənin smartfonuna və ya onun barmaq izinə sahib olmadığı üçün giriş cəhdi uğursuzluqla nəticələnir [1].

Eyni zamanda, MFA istifadəçiyə dərhal xəbərdarlıq edir: Tələbə daxil olmaq istəmədiyi halda telefonuna gələn təsdiq sorğusunu görərək şifrəsinin sındırıldığını anında başa düşür və təhlükəni bloklayaraq şifrəsini yeniləyir. Bu mexanizm statik şifrənin zəifliyini dinamik, zamana bağlı (TOTP - Time-based One-Time Password) və biometrik qatlarla əvəzləyərək mobil təhsildə akademik dürüstlüyü və fərdi məlumatların toxunulmazlığını 99.9% səviyyəsində təmin edir [1].

3. Texniki arxitektura və inteqrasiya modelləri. Mobil təhsildə MFA-nın effektivliyi yalnız onun mövcudluğu ilə deyil, onun Təhsil İdarəetmə Sistemlərinin (LMS) mürəkkəb arxitekturasına nə dərəcədə qüsursuz inteqrasiya olunması ilə ölçülür. Mobil ekosistemlərdə təhlükəsizlik protokolları server tərəfi (back-end), mobil tətbiq (front-end) və istifadəçi cihazı arasında asinxron və təhlükəsiz rabitəni təmin etməlidir.

3.1. MFA-nın üç fundamental komponenti və etibarlılıq iyerarxiyası. MFA arxitekturası təsadüfi seçilmiş faktorlar toplusu deyil, "etibarlılıq iyerarxiyası" üzərində qurulmuş elmi bir modeldir. Mobil təhsil mühitində

bu, adətən üç faktorun qarşılıqlı sintezi ilə həyata keçirilir:

- Bilmə faktoru (Knowledge - "Something you know"): Bu, autentifikasiyanın ən qədim və ən geniş yayılmış formasıdır. Bura mürəkkəb şifrələr, PİN kodlar və ya təhlükəsizlik sualları daxildir. Lakin mobil təhsildə bu faktor "statik" olduğu üçün təkbaşına zəif hesab edilir.
- Sahib olma faktoru (Possession - "Something you have"): Mobil təhsildə bu faktorun mərkəzində tələbənin smartfonu dayanır. Cihazın daxili təhlükəsizlik elementi (Secure Element) və ya "Trusted Platform Module" (TPM) unikal rəqəmsal imzaların saxlanılmasına imkan verir. Buraya həmçinin proqram təminatı əsaslı generatorlar (Authenticator tətbiqləri) daxildir.
- Mövcudluq faktoru (Inherence - "Something you are"): Bu, autentifikasiyanın ən yüksək səviyyəsidir. Biometrik göstəricilər (barmaq izi, FaceID, səs tanıma) istifadəçinin fiziki varlığını rəqəmsal olaraq təsdiqləyir.

Mobil platformalarda ən uğurlu və istifadəçi dostu model "Bilmə" (sadə bir PİN və ya şifrə) və "Mövcudluq" (biometrika) faktorlarının sintezidir. Bu sintez həm kiber-təhdidlərin qarşısını alır, həm də tələbənin mürəkkəb simvolları daxil etmək məcburiyyətini aradan qaldıraraq idarəetməni asanlaşdırır.

3.2. İnteqrasiya standartları: saml, oauth 2.0 və openıd connect. Müasir universitet infrastrukturları "parçalanmış" bir quruluşa malikdir; tələbələr bir seans ərzində həm imtahan portalına, həm elektron kitabxanaya, həm də video mühazirə bazasına müraciət edirlər. Bu sistemlərin hər birində MFA tələb etmək "autentifikasiya yorğunluğu" yaradır. Bunun həlli Single Sign-On (SSO) modelidir.

- SAML (Security Assertion Markup Language): XML əsaslı bu protokol universitetin mərkəzi İdentifikasiya Provayderi (IdP) ilə təhsil xidmətləri (Service Providers) arasında etibar körpüsü yaradır. Tələbə mobil tətbiq vasitəsilə bir dəfə MFA-dan keçdikdə, IdP digər bütün sistemlərə təhlükəsiz bir "təsdiq bildirişi" (assertion) göndərir. Bu, akademik resurslara giriş zamanı təhlükəsizliyi mərkəzləşdirir.
- OAuth 2.0 və OpenID Connect (OIDC): Müasir mobil tətbiqlərin (məsələn, Moodle Mobile və ya Canvas App) əksəriyyəti bu standartlara əsaslanır. OAuth 2.0 sistemə daxil olma səlahiyyətini (Authorization), OIDC isə şəxsiyyətin kimliyini (Authentication) idarə edir. Bu modeldə tələbənin şifrəsi heç vaxt mobil tətbiqin özündə saxlanılmır; sistem bunun əvəzinə müəyyən ömür müddəti olan "Access Token" və "Refresh Token"lərdən istifadə edir. Bu, cihaz oğurlanarsa, məlumatların sızma riskini minimuma endirir [5].

3.3. FIDO2 və şifrəsiz (Passwordless) təhsilin gələcəyi. Texnoloji arxitekturanın ən zirvə nöqtəsi FIDO2 (Fast IDentity Online) standartıdır. Bu, mobil təhsildə inqilabi bir sıçrayışdır, çünki o, şifrə anlayışını tamamilə ləğv etməyə imkan verir. FIDO2 "Public Key Cryptography" (Açıq açar kriptoqrafiyası) prinsipi ilə işləyir.

Tələbə öz mobil cihazındakı lokal biometrik kilidi (məsələn, FaceID) açdıqda, cihaz daxilində saxlanılan "gizli açar" vasitəsilə serverə rəqəmsal imza göndərilir. Serverdə isə yalnız "açıq açar" saxlanılır. Bu modelin ən böyük üstünlüyü ondan ibarətdir ki, universitetin serverləri sındırılsa belə, hücumçuların əlinə şifrə keçmir, çünki serverdə şifrə mövcud deyil. Bu, "Phishing" hücumlarını texniki olaraq imkansız hala gətirir.

3.4. Mobil inteqrasiyada API-lərin və SDK-ların texniki rolu. MFA həllərinin (məsələn, Google Authenticator, Duo Security və ya Microsoft Authenticator) təhsil platformalarına qoşulması RESTful API-lər vasitəsilə həyata keçirilir. Universitetin İT departamentləri tətbiqlərə xüsusi SDK (Software Development Kit) paketləri əlavə edərək autentifikasiya prosesini fərdiləşdirə bilərlər. Proses aşağıdakı kimi cərəyan edir:

1. Sorğu: Tələbə mobil tətbiqə giriş etmək istədikdə, tətbiq API vasitəsilə MFA serverinə sorğu göndərir.
2. Push Notification: MFA serveri tələbənin qeydiyyatdan keçmiş cihazına asinxron "Push" bildirişi göndərir.

3. Təsdiq: Tələbə barmaq izi ilə təsdiq verdikdə, SDK bu təsdiqi kriptoqrafik olaraq imzalayır və geri göndərir.
4. Giriş: Cavab müsbət olduqda, sistem "Session Token" yaradaraq tələbəyə təhsil materiallarına giriş icazəsi verir.

Bu asinxron iş rejimi o deməkdir ki, təhlükəsizlik yoxlaması təhsil prosesini "bloklamır" və internet sürətindən asılı olmayaraq fon rejimində sürətlə tamamlanır. Bu texniki arxitektura mobil təhsili həm kiber-qalaya çevirir, həm də müasir tələbənin gözlədiyi sürəti təmin edir.

4. Tələbə təcrübəsi və ux (user experıence). Mobil təhsildə (m-Learning) uğur yalnız texnoloji infrastrukturun gücü ilə deyil, həmin texnologiyanın son istifadəçi, yəni tələbə tərəfindən nə dərəcədə asanlıqla mənimsənilməsi ilə ölçülür. Kibertəhlükəsizlik tədbirləri çox vaxt istifadəçi təcrübəsinə (UX) maneə kimi görünsə də, müasir MFA həlləri bu stereotipi qırmaq məqsədi daşıyır.

4.1. Təhlükəsizlik və rahatlıq paradoksu: sürtünməsiz təhlükəsizlik (Frictionless Security). Rəqəmsal təhsil platformalarında ən böyük çətinliklərdən biri təhlükəsizlik tədbirləri ilə istifadəçi rahatlığı (UX) arasında "qızıl ortanı" tapmaqdır. Tədqiqatlar göstərir ki, müasir tələbə kontingenti, xüsusilə "Z nəsli" və "Alfa nəsli", rəqəmsal tətbiqlərdən anlıq reaksiya və minimum maneə gözləyirlər.

- 10 Saniyə qaydası: İnsan-kompüter qarşılıqlı əlaqəsi sahəsində aparılan araşdırmalar sübut edir ki, əgər hər hansı bir autentifikasiya prosesi 10 saniyədən artıq vaxt aparırsa, istifadəçinin fokuslanma dərəcəsi kəskin azalır və platformadan istifadə etmək istəyi zəifləyir. Mobil təhsildə bu, tələbənin öyrənmə axınından (learning flow) qopması deməkdir.
- Biometrikanın rolu: Ənənəvi şifrə daxil etmə prosesi "sürtünməli" (friction) bir prosesdir – istifadəçi klaviaturanı açmalı, şifrəni xatırlamalı və səhv etmədən daxil etməlidir. Lakin mobil cihazlardakı FaceID və ya barmaq izi skanerləri bu prosesi "sürtünməsiz" hala gətirir. MFA-nın düzgün tətbiqi əslində UX-i pisləşdirmir; əksinə, tələbəni uzun və mürəkkəb şifrələri xatırlamaq yükündən azad edərək, girişi bir toxunuşla mümkün edir.

4.2. Adaptiv autentifikasiya: süni intellektli və kontekstual təhlükəsizlik. İstifadəçi təcrübəsini təkmilləşdirən ən inqilabi yanaşmalardan biri Adaptiv (və ya Riskə Əsaslanan) Autentifikasiyadır. Bu sistem pərdəarxasında Süni İntellekt (AI) və Maşın Öyrənməsi (ML) alqoritmlərini işə salaraq, hər bir giriş cəhdini real vaxt rejimində analiz edir.

Sistem tələbənin davranış modelini (behavioral biometrics) və giriş kontekstini qiymətləndirmək üçün aşağıdakı parametrlərdən istifadə edir:

- Coğrafi məkan (Geo-location): Tələbə adətən dərslərinə Bakıdan qoşulursa və qəfil olaraq Londondan giriş cəhdi edilirsə, bu, yüksək risk siqnalıdır.
- Cihaz profili: Giriş tələbənin qeydiyyatdan keçmiş "iPhone" cihazındanmı, yoxsa naməlum bir "Windows" kompüterindənmi edilir?
- Zaman pəncərəsi: Tələbə adətən gündüz saatlarında aktivdirmi? Gecə saat 04:00-da edilən giriş cəhdi şübhəli hesab oluna bilər.
- IP ünvanı və şəbəkə: Tələbə universitetin şəbəkəsindədirmi, yoxsa şübhəli bir proxy/VPN istifadə edir?

Əgər bütün parametrlər tələbənin gündəlik davranış modeli ilə üst-üstə düşürsə, sistem riski "aşağı" qiymətləndirir və əlavə MFA sorğusu tələb etmədən (pasiv rejimdə) girişi təmin edir. Bu, tələbəni lüzumsuz bildirişlərlə yormadan maksimum təhlükəsizlik və rahatlıq təmin edir [7].

4.3. MFA yorğunluğu (MFA fatigue) və sosial mühəndisliklə mübarizə. Kibertəhlükəsizlik ədəbiyyatında yeni və təhlükəli bir termin yaranmışdır: "MFA Yorğunluğu". Kiberhücumçular istifadəçinin şifrəsini ələ keçirdikdən sonra, onun mobil cihazına ard-arda yüzlərlə push-bildirişi göndərirlər (Push Bombing). Hücumun məqsədi istifadəçini psixoloji cəhətdən yormaq və bezdirməkdir. Yorulmuş tələbə, sadəcə bu səsli bildirişlərin kəsilməsi üçün "Təsdiq et" düyməsinə basaraq bilmədən hücumçuya giriş icazəsi verə bilər [1]. Bu problemi kökündən həll etmək üçün

müasir UX dizaynında "Number Matching" (Rəqəm uyğunlaşdırma) metodu tətbiq olunur:

1. LMS giriş ekranında təsadüfi bir rəqəm (məsələn, "48") görünür.
2. Tələbənin mobil telefonuna gələn bildirişdə sadəcə "Təsdiq" düyməsi olmur; o, ekranda gördüyü həmin rəqəmi telefonuna daxil etməlidir.
3. Bu metod prosesi tamamilə avtomatizmdən (beyinsiz toxunuşdan) çıxarır və tələbənin şüurlu şəkildə prosesdə iştirakını təmin edir.

4.4. Davranış biometrikası: gələcəyin şəffaf təhlükəsizliyi. UX sahəsindəki növbəti addım Davranış Biometrikasıdır. Bu texnologiya tələbənin cihazdan necə istifadə etdiyini — ekrana toxunma təzyiqini, yazı sürətini, cihazı tutma bucağını və hərəkət ritmini analiz edir. Bu məlumatlar hər bir fərd üçün unikaldır. Gələcəkdə MFA sistemləri bu göstəricilər vasitəsilə tələbəni hələ o giriş düyməsinə basmadan tanıya biləcək. Bu, təhlükəsizliyin tamamilə "görünməz" olduğu və istifadəçi təcrübəsinin heç vaxt kəsilmədiyi mükəmməl bir rəqəmsal təhsil mühitinin yaradılmasına imkan verəcəkdir [4].

5. Mobil təhsildə təhlükəsizlik landşaftı. Mobil təhsilin (m-learning) ekosistemi, ənənəvi stasionar təhsil mühitindən fərqli olaraq, daha qeyri-mərkəzləşdirilmiş və dağınıq bir quruluşa malikdir. Bu dağınıqlıq, kibermüdafiə sərhədlərini genişləndirir və hər bir mobil cihazı potensial bir giriş nöqtəsinə çevirir. Təhlükəsizlik landşaftını anlamaq üçün biz üç əsas istiqaməti təhlil etməliyik: istifadəçi davranışı, hücum metodologiyaları və müdafiə mexanizmlərinin effektivliyi.

5.1. Zəif şifrə paradoksu: psixoloji və texniki analiz. Təhsil sektorunda kibertəhlükəsizliyin ən zəif halqası, adətən, texnologiyanın özü deyil, həmin texnologiyadan istifadə edən insandır. Tələbə kontingenti arasında aparılan sorğular göstərir ki, rəqəmsal savadlılıq yüksək olsa da, "təhlükəsizlik gigiyenası" eyni səviyyədə deyil.

- Şifrə təkrarı (Password Reuse): Tələbələrin təxminən 73%-i onlayn bankçılıq, sosial media və universitet portalı kimi müxtəlif əhəmiyyətli platformalarda eyni və ya çox bənzər şifrələrdən istifadə edir. Bu, bir platformanın sındırılması halında zəncirvari reaksiya yaradır.
- Şifrə mürəkkəbliyi vs. mobil rahatlıq: Mobil cihazlarda klaviatura interfeysi mürəkkəb simvolların daxil edilməsini (məsələn: *, &, ^, %) çətinləşdirir. Bu fiziki məhdudiyyət tələbələri şüuraltı olaraq daha sadə, rəqəm və hərflərdən ibarət şifrələrə yönəldir.
- İqtisadi təsir: IBM-in "Məlumat sızmasının dəyəri" (Cost of a Data Breach) hesabatına görə, təhsil müəssisələrində bir tək sızmanın orta xərci milyonlarla dollarla ölçülür. Bu xərcin böyük bir hissəsi məhz zəif şifrələr vasitəsilə baş verən ilkin daxilolmaların nəticəsidir.

5.2. Kiberhücumların təkamülü: mobil təhsilin hədəfə alınması. Kibercinayətkarlar mobil təhsil platformalarının xüsusiyyətlərini nəzərə alaraq öz metodologiyalarını inkişaf etdirmişlər.

a) Mobil Phishing (Smishing və Vishing): Ənənəvi e-poçt fishing-i mobil mühitdə daha təhlükəli formalara çevrilmişdir. Mobil cihazlarda ekran ölçüsü məhdud olduğu üçün brauzerin ünvan sətrindəki URL-in həqiqiliyini yoxlamaq çətindir. Hücumçular tələbələrə SMS vasitəsilə "İmtahan nəticələriniz açıqlandı" və ya "Təqaüd ödənişi üçün təsdiq lazımdır" kimi təcili xarakterli mesajlar göndərirlər. Tələbə təşviş içində linkə daxil olduqda, qarşısına universitetin LMS (Learning Management System) portalının mükəmməl saxta nüsxəsi çıxır [8].

b) Credential Stuffing və Botnetlərin Rolu: Bu hücum növü "kütləvi sınaq" prinsipinə dayanır. Hücumçular qara bazardan əldə etdikləri milyonlarla istifadəçi məlumatını avtomatlaşdırılmış botlar vasitəsilə universitet portallarına tətbiq edirlər. Mobil təhsil tətbiqlərinin API-ləri (Application Programming Interface) çox vaxt bu cür sürətli daxilolma cəhdlərini bloklamaq üçün kifayət qədər "rate-limiting" (sürət məhdudiyyəti) funksiyasına malik olmur.

c) Man-in-the-Middle (MitM) və İctimai Wi-Fi: Tələbələr dərslərə və onlayn materiallara çox vaxt kafelərdə, kitabxanalarda və ya nəqliyyatda olan pulsuz və təhlükəsiz olmayan Wi-Fi şəbəkələri üzərindən daxil olurlar. Bu şəbəkələrdə hücumçular trafiki izləyərək

tələbənin sessiya tokenlərini (session tokens) ələ keçirə bilərlər.

5.3. MFA-nın dinamik müdafiə mexanizmi: çoxqatlı təhlükəsizlik. MFA bu hücumların qarşısını almaq üçün "Defense in Depth" (Dərindən Müdafiə) fəlsəfəsini tətbiq edir. Bu fəlsəfəyə görə, təhlükəsizlik bir deyil, bir neçə müstəqil səddən ibarət olmalıdır.

1. Hücumun iqtisadi səmərəsizləşdirilməsi: Kiberhücumların böyük hissəsi avtomatlaşdırılıb. MFA tətbiqi hücumun mürəkkəbliyini artırır. Əgər bir hücumçu şifrəni ələ keçirsə belə, ikinci faktorun (məs., tələbənin telefonundakı biometrik təsdiq) ələ keçirilməsi fərdi müdaxilə tələb edir ki, bu da kütləvi hücumları iqtisadi baxımdan səmərəsiz edir.
2. Dinamiklik və zaman məhdudiyyəti: MFA vasitəsilə təqdim olunan birdəfəlik kodlar (OTP) adətən Time-based One-Time Password (TOTP) alqoritmi ilə işləyir. Bu kodlar 30 saniyədən bir yenilənir. Bu o deməkdir ki, hücumçu kodu ələ keçirsə belə, ondan istifadə etmək üçün cəmi bir neçə saniyəsi var [5].
3. Cihaz və ıdentiklik harmoniyası: Mobil təhsildə MFA, cihazı tələbənin rəqəmsal şəxsiyyətinin fiziki bir parçasına çevirir. Universitetin sistemi təkcə "nə yazıldığını" deyil, həm də girişin "hansı cihazdan" edildiyini yoxlayır. Bu, saxta profil girişlərini demək olar ki, qeyri-mümkün edir [5].

5.4. Statistik göstəricilər və real case study. Dünya üzrə aparılan araşdırmalar göstərir ki, MFA-nın tətbiqi hesabların ələ keçirilməsi (account takeover) riskini 99.9% azaldır. Məsələn, 2021-ci ildə bir ABŞ universiteti bütün tələbə və müəllim heyəti üçün məcburi MFA tətbiqinə keçdikdən sonra fishing şikayətlərinin sayının 85% azaldığını müşahidə etmişdir. Bu, MFA-nın sadəcə texnoloji bir əlavə olmadığını, həm də institusional kibertəhlükəsizlik mədəniyyətini necə kökündən dəyişdiyini göstərir [2].

6. Nəticə və gələcək perspektivlər

6.1. Strateji zərurət və rəqəmsal etibar. Tədqiqatımız göstərir ki, mobil təhsilin (m-learning) sürətli inkişafı təhsil müəssisələrini kritik bir seçim qarşısında qoymuşdur: ya təhlükəsizlikdən güzəştə gedərək sadə daxilolma mexanizmlərini saxlamaq, ya da Çoxfaktorlu Autentifikasiya (MFA) vasitəsilə rəqəmsal etimad mühiti qurmaq. Bu gün MFA tətbiqi sadəcə texnoloji bir əlavə və ya seçim deyil; bu, təhsilin davamlılığını təmin edən strateji bir zərurətdir. Məqalə boyunca analiz etdiyimiz texniki arxitektura və istifadəçi təcrübəsi modelləri sübut edir ki, MFA təhsil ekosistemindəki təhlükəsizlik boşluqlarını doldurmaqla yanaşı, həm də rəqəmsal öyrənmə prosesini daha peşəkar və legitim müstəviyə daşıyır.

6.2. Kiber-dayanıqlıq: hücumdan qorunma deyil, müdafiə mədəniyyəti. Universitetlərin kiber-dayanıqlığı artıq yalnız serverlərin gücü ilə deyil, hər bir tələbənin və müəllimin rəqəmsal identifikasiyasının necə qorunması ilə ölçülür. MFA-nın tətbiqi phishing, credential stuffing və kütləvi bot hücumları kimi müasir təhdidlərin effektivliyini minimuma endirir. Lakin bu müvəffəqiyyət yalnız texniki tətbiqlə bitmir; MFA həm də istifadəçilərdə "kiber-məsuliyyət" hissini formalaşdırır. Tələbə hər dəfə öz smartfonuna gələn bildirişi təsdiqlədikdə, rəqəmsal identikliyinə sahib çıxmaq vərdişi qazanır. Bu, təhsil müəssisəsini passiv qorunmadan aktiv müdafiə mədəniyyətinə keçirir [9].

6.3. İnsan mərkəzlilik və adaptiv gələcək. Gələcəyin təhlükəsizlik modelləri istifadəçini "yormayan" texnologiyalar üzərində qurulacaqdır. Adaptiv autentifikasiya və süni intellekt dəstəkli risk analizi göstərir ki, təhlükəsizlik nə qədər "görünməz" olarsa, onun qəbul edilməsi bir o qədər asan olar. İnsan mərkəzli yanaşma, tələbənin akademik axınına mane olmadan, onu arxa fonda qoruyan ağıllı alqoritmlərin tətbiqini tələb edir. Bu, təkcə texnoloji rahatlıq deyil, həm də rəqəmsal transformasiyanın humanistləşməsi prosesidir.

6.4. İnstitusional nüfuz və akademik dürüstlük. Rəqəmsal transformasiya şəraitində universitetlərin verdiyi təhsilin və rəqəmsal dərəcələrin dəyəri birbaşa həmin müəssisənin infrastrukturunun təhlükəsizlik səviyyəsi ilə əlaqəlidir. MFA ilə qorunmayan bir platformada verilən imtahan və ya alınan diplom, kənar müdaxilələrə açıq olduğu üçün akademik etibarını itirə bilər. Buna görə də, təhsil müəssisələri MFA-nı yalnız İT şöbəsinin məsələsi

kimi deyil, akademik keyfiyyət və institusional nüfuzun qorunması mexanizmi kimi görməlidirlər.

6.5. Gələcəyə baxış: şəffaf və fasiləsiz autentifikasiya. Məqalənin sonunda vurğulamaq lazımdır ki, biz hazırda "interaktiv MFA" mərhələsindəyik (kod daxil etmə və ya düyməyə basma). Lakin süni intellektin (AI) və neyron şəbəkələrinin daha da dərinləşməsi ilə biz "Davranış Biometrikası" (Behavioral Biometrics) dövrünə qədəm qoyuruq. Gələcəkdə MFA sistemləri tələbənin:

- Smartfonu tutma bucağını,
- Ekrana toxunma təzyiqini,
- Yazı sürətini və ritmini,
- Naviqasiya vərdişlərini analiz edəcəkdir.

Bu sistemlər heç bir kod və ya bildiriş tələb etmədən, istifadəçinin həqiqətən kim olduğunu fasiləsiz şəkildə yoxlayacaq. Beləliklə, təhlükəsizlik tamamilə şəffaf (invisible security) hala gələcək və mobil təhsil həm ən yüksək müdafiə səviyyəsinə, həm də ən mükəmməl istifadəçi təcrübəsinə çatacaqdır. Bu inqilab, təhsilin gələcəyini daha inklüziv, daha əlçatan və ən əsası, daha təhlükəsiz edəcəkdir.

ƏDƏBİYYAT SİYAHISI

1. Das A.K., Wazid M., Kumar N., Khan M.K., Choo K.K.R., Park Y.H. A secure and robust multi-factor user authentication scheme for cloud computing environments. International Journal of Communication Systems, 2018;31(9): e3539. Doi: 10.1002/dac.3539
2. Grech A., Camilleri A.F. Blockchain in Education. European Commission, Joint Research Centre (JRC) Science for Policy Report. 2017.
3. Hardt D. The OAuth 2.0 Authorization Framework. IETF RFC 2012;6749. Doi: 10.17487/RFC6749
4. Holden O.L., Norris M.E., Kuhlmeier V.A. Academic ıntegrity in online assessment: A research review. Frontiers in Education, 2021;6:639814. Doi: 10.3389/feduc.2021.639814
5. O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 2003;91(12):2021–2040. Doi: 10.1109/JPROC.2003.819611
6. Traxler J. Defining, designing and delivering mobile learning. International Review of Research in Open and Distributed Learning, 2007;8(2). Doi: 10.19173/irrodl.v8i2.346
7. UNESCO. Guidelines for ICT in Education Policies and Masterplans. Paris: UNESCO Publishing. 2022.
8. Google Scholar elmi verilənlər bazası: Autentifikasiya və təhlükəsizlik standartları üzrə resurslar. URL: https://scholar.google.com
9. IEEE Xplore Digital Library: Texniki arxitektura və şəbəkə siyasətlərinin (Network Policies) idarə olunması üzrə elmi tədqiqatlar. URL: https://ieeexplore.ieee.org

Orkhan Vagif KAZIMOV
Master's student at Information Systems in Management, Western Caspian University

BUILDING TRUST IN DIGITAL EDUCATION: TECHNICAL ARCHITECTURE AND STRATEGIC ADVANTAGES OF MFA IN MOBILE LEARNING PLATFORMS

Summary

While the rapid integration of mobile technologies into the education sector has freed the learning process from the constraints of time and space, it has simultaneously created significant cybersecurity vulnerabilities. This article explores the mechanisms for implementing Multi-Factor Authentication (MFA) to protect user data and ensure academic integrity within mobile learning (m-learning) ecosystems. The research analyzes the integration architecture of MFA into cloud-based Learning Management Systems (LMS), the technical advantages of biometric identification methods,

and the impact of this technology on student user experience (UX). The article emphasizes that MFA is not only a tool for protection against cyberattacks but also a strategic element that preserves the institutional reputation of educational entities in the era of digital transformation. Finally, the study proposes adaptive and user-friendly authentication models for mobile learning platforms.

Keywords: Mobile learning, MFA, cybersecurity, digital transformation, biometric authentication.

Орхан Вагиф КАЗИМОВ
Магистр по Информационным Системам в Управлении, Западно-Каспийский Университет

ПОСТРОЕНИЕ ДОВЕРИЯ В ЦИФРОВОМ ОБРАЗОВАНИИ: ТЕХНИЧЕСКАЯ АРХИТЕКТУРА И СТРАТЕГИЧЕСКИЕ ПРЕИМУЩЕСТВА MFA В МОБИЛЬНЫХ ПЛАТФОРМАХ ОБУЧЕНИЯ

Резюме

Стремительная интеграция мобильных технологий в сектор образования освободила процесс обучения от ограничений времени и пространства, но в то же время создала серьезные уязвимости в кибербезопасности. В данной статье исследуются механизмы внедрения многофакторной аутентификации (MFA) для защиты пользовательских данных и обеспечения академической честности в экосистемах мобильного обучения (m-learning). В рамках исследования анализируются архитектура интеграции MFA в облачные системы управления обучением (LMS), технические преимущества методов биометрической идентификации и влияние этой технологии на пользовательский опыт (UX) студентов. В статье подчеркивается, что MFA является не только средством защиты от кибератак, но и стратегическим элементом, поддерживающим институциональную репутацию образовательных учреждений в эпоху цифровой трансформации. В завершение исследования предлагаются адаптивные и удобные для пользователя модели аутентификации для мобильных платформ обучения.

Ключевые слова: мобильное обучение, MFA, кибербезопасность, цифровая трансформация, биометрическая аутентификация.

Daxil olub: 22.04.2026