

ONLAYN TEST TIZIMLARIDA AMALDA QO'LLANILAYOTGAN XAVFSIZLIK CHORALARI

Miyassarov Javlonbek Mag'ripovich

*Muhammad al-Xorazmiy nomidagi ixtisoslashtirilgan maktab Samarqand fililali ijrochi
direkoti*

MAQOLA MALUMOTI

ANNOTATSIYA:

MAQOLA TARIXI:

Received: 03.11.2025

Revised: 04.11.2025

Accepted: 05.11.2025

KALIT SO'ZLAR:

*test, onlayn, tizim,
integratsiya, baza,
versiya, nazorat, zaxira,
nusxa.*

Ushbu maqolada onlayn test tizimlarida amalda qo'llanilayotgan xavfsizlik choralari hamda ularning ishlash mexanizmlari haqida so'z brogan bo'lib, maqola orqali onlayn test tizimlarining zaif nuqtalarini aniqlash, test natijalarining yaxlitligini ta'minlashda esa ma'lumotlar bazasining huquqiy integriteti (Integrity Constraints), versiya nazorati va zaxira nusxalarning mavjudligi haqida ham batafsil so'z yuritilgan.

Kirish

Zamonaviy ta'lim muassasalarida keng qo'llanilayotgan onlayn test tizimlari o'z ichiga axborot almashinuvi, test sinovlarini uzatish, ma'lumotlarni saqlash va foydalanuvchilar o'rtasida autentifikatsiya kabi funksiyalarni jamlagan bo'lib, bu jihatlar axborot xavfsizligining kompleks yondashuvini talab etadi. Platforma orqali amalga oshiriladigan testlash jarayonida ishtirok etayotgan foydalanuvchilarning shaxsiy ma'lumotlari, test mazmuni va natijalari himoyasiz qolgan taqdirda, ularning maxfiyligi, butunligi yoki mavjudligi buzilishi ehtimoli yuqori bo'ladi. Shu sababli, amaliyotda test tizimlarining xavfsizligini ta'minlashda bir nechta texnik chora-tadbirlar kompleksi joriy etiladi.

Dastlab, onlayn test tizimlarining zaif nuqtalari aniqlanib, ularga nisbatan mos himoya mexanizmlari ishlab chiqiladi. Bu borada xalqaro axborot xavfsizligi standartlariga (masalan, ISO/IEC 27001) va veb-ilovalar xavfsizligiga oid OWASP Top 10 tavsiyalariga tayanish amaliyotda eng samarali yondashuvlardan biri hisoblanadi [26,27].

Birinchi navbatda, foydalanuvchi autentifikatsiyasi tizimning xavfsizligi uchun poydevor bo'lib xizmat qiladi. Klassik parol asosidagi autentifikatsiya usullarining kuchsizligi sababli ko'plab tizimlarda ko'p bosqichli autentifikatsiya (Multi-Factor Authentication – MFA) joriy qilinmoqda. Bunda foydalanuvchidan nafaqat parol, balki vaqtinchalik SMS-kod, biometrik parametr yoki maxsus qurilmadagi tasdiqlash orqali tizimga kirishga ruxsat beriladi [28]. Shuningdek, biometrik autentifikatsiyaning, ayniqsa yuzni aniqlashga asoslangan Face-ID texnologiyasining joriy etilishi, aynan test topshirayotgan shaxsning o'zini aniqlash imkonini beradi. Bu nafaqat shaxsni tanib olishning aniqroq usulidir, balki parollar o'g'irlanishining oldini olishda ham foydalidir.

Foydalanuvchilarga berilgan rollarga asoslangan huquqlarni boshqarish (Role-Based Access Control – RBAC) orqali test mazmuni, ballar va tahrir qilish imkoniyatlarini faqat tegishli foydalanuvchilargagina taqdim etish mumkin. Administrator, o'qituvchi va o'quvchi rollari orasidagi funktsional farqlar aniqlik bilan belgilanmasa, huquq buzilishlari yuzaga keladi. Masalan, o'quvchining javoblarini tahrirlash imkoniyatiga ega bo'lmasligi, test muallifining esa faqat o'ziga tegishli testlarni boshqarish imkoniyatiga ega bo'lishi kerak [29].

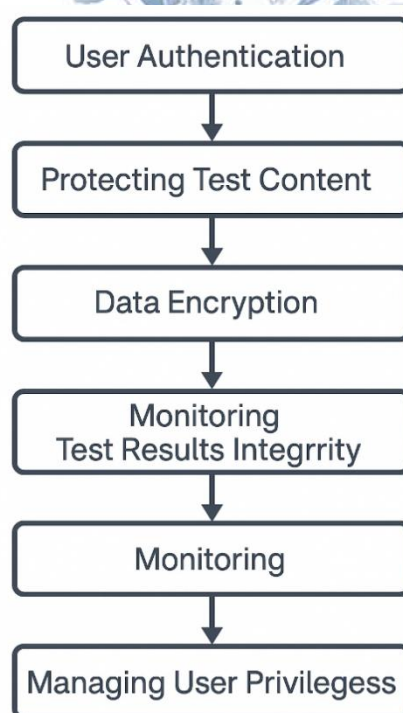
Test mazmunini himoya qilishda shifrlash algoritmlari muhim rol o'ynaydi. Ma'lumotlar saqlash jarayonida (Data at Rest) hamda uzatish jarayonida (Data in Transit) himoyalaniishi kerak. SSL/TLS protokollari asosida amalga oshirilgan shifrlash, foydalanuvchi va server o'rtasida yuborilayotgan ma'lumotlarning ushlanib qolishini oldini oladi. Bundan tashqari, test savollari va javob variantlarining bazada shifrlangan ko'rinishda saqlanishi – hatto administrator darajasidagi foydalanuvchining test mazmunini ko'rishini cheklash imkonini beradi. Ushbu yondashuv orqali testlar kontenti maxfiyligi kafolatlanadi, ayniqsa, attestatsion testlar yoki tanlovlarda bu juda muhim hisoblanadi.

Test natijalarining yaxlitligini ta'minlashda esa ma'lumotlar bazasining huquqiy integriteti (Integrity Constraints), versiya nazorati va zaxira nusxalarning mavjudligi muhim rol o'ynaydi. Ba'zi hollarda test javoblarining noto'g'ri tahrirlanishi yoki noto'g'ri saqlanishi yuzaga keladi. Bunday holatlarning oldini olish uchun tranzaktsiyalar asosida ishlaydigan ma'lumotlar bazasi boshqaruv tizimlari (masalan, PostgreSQL) va avtomatlashtirilgan backup tizimlari joriy etiladi [30].

Onlayn test jarayonining monitoringi uchun foydalanuvchilarning xatti-harakatlarini nazorat qilish vositalari muhim ahamiyat kasb etadi. Bu monitoring foydalanuvchining test davomida boshqa sahifalarga o'tishini, test oynasidan chiqib ketishini, bir vaqtning o'zida

bir nechta qurilmadan foydalanishini aniqlash imkonini beradi. Amalda, ushbu monitoring tizimi veb-brauzerga integratsiyalashgan maxsus JavaScript agentlari yoki serverda saqlanuvchi log tahlillari yordamida amalga oshiriladi. Ba'zi hollarda, veb-kamera orqali foydalanuvchini kuzatish, test davomida yuz ifodalarini aniqlash, hatto kognitiv yuklama asosida stress darajasini baholash imkonini beruvchi vositalar ham sinovdan o'tkazilgan. Shu bilan birga, foydalanuvchining holatini sun'iy intellekt yordamida tahlil qiluvchi proktorlik tizimlari (AI-proctoring) bugungi kunda keng joriy qilinmoqda [31].

Yuqorida ta'kidlangan har bir chorani vizual ko'rinishda quyidagi shaklda aks ettirish mumkin (2.1-rasm).



2.1-rasm. Onlayn test tizimida xavfsizlik qatlamlari arxitekturası

Monitoring tizimi faol ishlatilgan onlayn test platformalarida foydalanuvchi faoliyatini real vaqtda kuzatish tizimining samaradorligi isbotlangan. Shu jihatdan, foydalanuvchining sichqoncha harakatlari, klaviatura bosishlari, brauzer fokusining aktiv holatidan chiqib ketgan vaqti aniqlanadi. Bunday tizimlar ayniqsa test topshiruvchilarning biror vaqtda boshqa sahifalarga o'tishini yoki mobil qurilmalar orqali yordam so'rashini aniqlashda yordam beradi. Bu monitoring mexanizmlarining natijalari serverda log fayllar sifatida saqlanadi, keyin esa avtomatik tahlilga yuboriladi. Agar bir nechta shubhali xatti-harakatlar

aniqlansa, tizim test topshiruvchini ogohlantirishi yoki testni avtomatik to'xtatib qo'yishi mumkin.

Monitoringga oid yechimlar hozirgi kunda proktorlik xizmatlari bilan birlashtirilmoqda. Proktorlik – bu inson tomonidan yoki sun'iy intellekt yordamida foydalanuvchining testdagi harakatlarini real vaqt rejimida kuzatish tizimidir. Inson proktorlik amaliyotda cheklangan sonli test topshiruvchilar uchun ishlatiladi, ammo keng ko'lamli onlayn testlarda bu samarasiz hisoblanadi. Shu sababli, AI-proktorlik tizimlari, masalan, Respondus Monitor yoki ProctorU kabi tizimlar foydalanuvchining yuz ifodasi, qarash yo'nalishi, gapirish yoki boshqa birov bilan muloqotga kirishish holatlarini tahlil qilib, shubhali hatti-harakatlarni avtomatik belgilab boradi [32].

Axborotni himoyalashda muhim bosqichlardan yana biri bu DLP – Data Loss Prevention (Ma'lumotlar yo'qotilishini oldini olish) texnologiyalaridir. Bu turdagi tizimlar server, ilova va foydalanuvchi sathida amalga oshirilgan barcha ma'lumotlar almashinuvini kuzatadi va ma'lum xavf darajasiga ega ma'lumotlarning ruxsatsiz ko'chirilishiga yo'l qo'ymaydi. Masalan, test natijalari fayl sifatida eksport qilinayotganda, agar bu harakat maxsus avtorizatsiyadan o'tmagan bo'lsa, tizim uni bloklashi yoki faqat shifrlangan holda saqlashga ruxsat berishi mumkin. Shu tarzda test natijalari, foydalanuvchi ballari yoki statistik hisobotlarning sizib chiqish ehtimoli kamayadi.

Foydalanuvchi xatti-harakatlarining avtomatik tahlili tizimdagi turli xavfsizlik choralarini samarali nazorat qilishda muhim omil bo'lib xizmat qiladi. Har bir foydalanuvchi kirish va chiqish vaqtlarining to'liq loglari, sahifa o'zgarishlari, testdagi savollarga ajratilgan vaqtlar, shubhali qadamlar, ishlatilgan qurilmalar IP-manzillari va geolokatsiyasi kabi ko'rsatkichlar asosida xavf darajasi profili hosil qilinadi. Ushbu profilga asosan tizim har bir foydalanuvchining testdagi ishtirokini xavfsizlik nuqtai nazaridan baholaydi. Misol uchun, bir foydalanuvchi test davomida 5 marta brauzerni minimallashtirgan, kameraga qaramagan va test oynasidan chiqib turgan bo'lsa, u foydalanuvchiga "o'rtacha xavf" statusi berilishi mumkin. Bu metodika ayniqsa sun'iy intellekt asosida yaratilgan tizimlarda qo'llaniladi [33].

Bunday choralarni amalga oshirishda platforma ishlab chiquvchilari tomonidan nafaqat texnik himoya, balki foydalanuvchilarning shaxsiy hayotini hurmat qilish borasida ham muvozanatni saqlash zarur. Foydalanuvchilarga monitoring, kamera orqali kuzatuv va log yozuvlar borasida oldindan ruxsatnoma (consent form) taklif etilishi, ma'lumotlar qay darajada yig'ilishi va qancha muddat saqlanishi haqida aniq axborot taqdim etilishi xalqaro

axborot maxfiyligi siyosatlariga muvofiqligini ta'minlaydi.

Quyida amalda keng tarqalgan xavfsizlik choralari va ularning asosiy jihatlarini qiyoslaydigan jadval taqdim etilgan (2.1-jadval).

2.1-jadval. Onlayn test tizimlarida qo'llanilayotgan xavfsizlik choralari va ularning xususiyatlari

Chora nomi	Asosiy vazifasi	Afzalliklari	Cheklovlari
Foydalanuvchi autentifikatsiyasi	Shaxsni aniqlash va huquq berish	Soddalik, MFA imkoniyati	Parol buzilishi ehtimoli
Shifrlash (SSL/TLS)	Ma'lumotlarni uzatishda himoya qilish	Yashirin kanal, trafikning himoyalanganligi	Sertifikatlar muddati cheklangan
Proktorlik (AI asosida)	Test topshiruvchini real vaqtda kuzatish	Sun'iy intellekt yordamida aniqlik	Kamera kerak, shaxsiy hayot talabi
DLP texnologiyalari	Ma'lumotlar sizib chiqishini oldini olish	Ma'lumotlar oqimini to'liq nazorat qilish imkoniyati	Katta tizim resurslari talab qiladi
Foydalanuvchi xatti-harakatlari tahlili	Xavf darajasini aniqlash	Profilga asoslangan xavf modeli	Noaniqlik holatlari mumkin
Monitoring va loglash	Tizimdagi barcha harakatlarni qayd etish	Audit va tekshiruvlar uchun hujjatlashtirilgan ma'lumotlar	Katta hajmli saqlash muammosi

Ushbu jadvaldan ko'rinib turibdiki, har bir xavfsizlik chorasi o'ziga xos afzallik va cheklovlarga ega. Shuning uchun amaliyotda ularni integratsiyalashgan holda, bir-birini to'ldiruvchi mexanizmlar sifatida qo'llash eng maqbul yondashuv hisoblanadi.

Foydalanilgan adabiyotlar

1. Online Exam Cheating Is Up. Tom Williams for Times Higher Education. April 27, 2022.
2. DDoS attacks against educational resources increased by more than 350% this spring.

Kaspersky. September 4, 2020

3. Digital Education: The cyberrisks of the online classroom. 04 Sep 2020

4. China Deploys AI, Facial Recognition to Deter Exam Cheats. By Ding Rui. Jun 06, 2024

5. Mitchell Clark. Students of color are getting flagged to their teachers because testing software can't see them. Apr 9, 2021.

6. William Crumpler. How Accurate are Facial Recognition Systems – and Why Does It Matter? SCIC. April 14, 2020

7. Robiya Yoldosheva. Biometrik xavfsizlik – shaxs yuzni aniqlash va tasdiqlash. Texnokun.uz. 28.10.2022.

8. Ravinder Punia, Kailash Bahl. Online Examination System –Architecture. IJISSET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017.

9. Guizhen Wang. Design of a Student's Online Examination System Based on B/S Architecture. 2016 International Seminar on Education, Innovation and Economic Management (SEIEM 2016)

10. Michelle Rossevelt. Protecting Student Data in Online Testing: Security Measures and Future Trends. Data Security. November 21, 2023

11. Smart Assessment Solutions: Navigating the Future of Modern Online Examination Systems. Team Creatrix. February 20, 2024

12. Baltum Buro. ISO/IEC 27001 Axborot xavfsizligini boshqarish tizimining afzalliklari. Oktabr 10, 2016 baltumburoo.com

13. OWASP Top Ten 2025. Top 10 Web Application Security Risks. <https://owasp.org/>

14. STRIDE model. <en.wikipedia.org>

15. Comparison of STRIDE, DREAD & PASTA. By Sherif Koussa. www.softwaresecured.com

16. DREAD (risk assessment model). <en.wikipedia.org>

17. Windows Hello face authentication. Microsoft.com. 07/15/2021

18. Azmath Moosa. A Comprehensive Guide to Facial Recognition Algorithms - Part 1. BaseApp. May 28, 2018

19. Milestones in Facial Recognition Technology: A Historical Overview. FacitAI. 4 November 2024.

20. Gonzalo Benito. Comparing classical and deep approaches for face recognition in a smartgym application. MASTER THESIS DISSERTATION, MASTER IN COMPUTER VISION, JULY 2017