INTERFAOL O‘QUV PLATFORMADA FOYDALANUVCHI AUTENTIFIKATSIYASI VA RBAC MEXANIZMINI JORIY ETISH

Masharipov Dilmurod Atanazarovich
Osiyo xalqaro universiteti, Ijtimoiy Fanlar va texnologiyalar fakulteti,
magistratura talabasi, Urgench, Uzbekistan
masharipovdilmurod52@gmail.com

Annotatsiya: Ushbu tezisda interfaol o‘quv platformalarida foydalanuvchilarni autentifikatsiya qilish va rollarga asoslangan kirish nazorati (RBAC)ni joriy etishning texnik jihatlari IMRaD strukturasi asosida ko‘rib chiqiladi. Platforma arxitekturasi frontend, backend va ma’lumotlar bazasi qatlamlaridan iborat bo‘lib, ularda OpenID Connect, JWT (JSON Web Token) va RBAC modeli integratsiyalashgan. Frontend foydalanuvchining ro‘yxatdan o‘tishi, tizimga kirishi va roli kodlangan JWT tokenni qabul qilishini ta’minlaydi, backend esa parolni xeshlash, ikki bosqichli autentifikatsiya (2FA) va token generatsiyasi uchun mas’uldir. Ma’lumotlar bazasida Users, Roles, Permissions, User_Roles va Role_Permissions jadvallari orqali “Admin”, “Teacher”, “Student” va “Guest” rollari uchun vakolatlar formal tarzda boshqariladi. Taklif etilgan yechim “least privilege” tamoyilini ta’minlab, himoyalangan API endpointlar uchun ruxsatlarni tekshirish hamda audit imkoniyatlari orqali interfaol ta’lim platformalarida axborot xavfsizligi va boshqaruv samaradorligini oshiradi.

Kalit so‘zlar: Autentifikatsiya, Avtorizatsiya, RBAC, OpenID Connect, JWT, 2FA, Interfaol o‘quv platforma, Foydalanuvchi rollari, Axborot xavfsizligi, Ma’lumotlar bazasi modeli.

Kirish

Raqamli ta’lim infratuzilmasining kengayishi natijasida interfaol o‘quv platformalarida foydalanuvchilarni ishonchli autentifikatsiya qilish va ularga beriladigan vakolatlarni qat’iy nazorat qilish zaruriyati keskin ortib bormoqda. Bunday platformalarda autentifikatsiya foydalanuvchining shaxsini aniqlash jarayoni bo‘lsa, rollarga asoslangan kirish nazorati (RBAC) unga ruxsat etilgan funksiyalar doirasini formal tarzda belgilaydi. O‘qituvchi, talaba, administrator va mehmon (guest) kabi turli rollarning bir xil axborot tizimida faoliyat yuritishi xavfsizlik siyosatini tizimli loyihalashni talab qiladi.

Ushbu tezisda interfaol o‘quv platformasi uchun OpenID Connect, JWT va RBAC elementlarini birlashtirgan uch qatlamli arxitektura asosida autentifikatsiya va avtorizatsiya mexanizmlari yoritiladi. Tizim Users, Roles, Permissions, User_Roles va Role_Permissions jadvallari orqali foydalanuvchi–rol–ruxsat zanjirini ifodalashga qaratilgan bo‘lib, bu texnika yo‘nalishi talabalari va axborot xavfsizligi mutaxassislari uchun amaliy ahamiyatga ega. Tadqiqotning maqsadi – interfaol o‘quv platformasida xavfsiz seans boshqaruvi, rollarga asoslangan kirish nazorati va audit imkoniyatlarini yagona arxitektura doirasida asoslash va tavsiflashdan iborat.

Metodlar

Tadqiqot metodologiyasi uch qatlamli dasturiy arxitektura – frontend, backend va ma'lumotlar bazasi – asosida qurilgan bo'lib, har bir qatlam autentifikatsiya va avtorizatsiya jarayonida o'ziga xos funksiyani bajaradi. Frontend (Web/Mobile UI) foydalanuvchi bilan bevosita muloqot qiluvchi qism bo'lib, ro'yxatdan o'tish, tizimga kirish, 2FA kodlarini kiritish hamda autentifikatsiyadan keyin olingan JWT tokenni saqlash va so'rovlar bilan birga yuborish vazifasini bajaradi. Foydalanuvchi roli va ruxsatlariga qarab menyu elementlari dinamik generatsiya qilinadi, ya'ni administrator uchun boshqaruv bo'limlari, o'qituvchi uchun kurslarni boshqarish, talabalar uchun esa o'quv materiallari va testlar ko'rinadi.

Backend qismida API Gateway va Auth Service modullari asosiy rol o'ynaydi. API Gateway barcha tashqi HTTP(S) so'rovlarni markazlashtirilgan tarzda qabul qilib, autentifikatsiya va avtorizatsiya qoidalariga mos ravishda tegishli mikroservislarga yo'naltiradi. Auth Service foydalanuvchini ro'yxatdan o'tkazish, parolni bcrypt yoki SHA-256 algoritmlari asosida salt bilan xeshlash, login jarayonida kiritilgan ma'lumotlarni tekshirish, 2FA (Email/SMS OTP yoki TOTP) ni ishga tushirish hamda JWT va refresh tokenlarni generatsiya qilish funksiyalarini bajaradi. JWT token header, payload va HMAC-SHA256 imzodan iborat bo'lib, payload ichida foydalanuvchi identifikatori, roli va token amal qilish muddati saqlanadi.

Ma'lumotlar bazasi sathida RBAC modelini implementatsiya qilish uchun Users, Roles, Permissions, User_Roles, Role_Permissions va Login_Logs jadvallari ishlatiladi. Users jadvali foydalanuvchilarning shaxsiy ma'lumotlari va xeshlangan parollarini saqlasa, Roles jadvali tizimdagi rollar to'plamini (Admin, Teacher, Student, Guest va boshqalar) ifodalaydi. User_Roles jadvali foydalanuvchi–rol munosabatini, Role_Permissions esa rol–ruxsat bog'lanishini belgilaydi va shu orqali "bu foydalanuvchi nima qila oladi?" savoliga formal javob shakllanadi. Login_Logs jadvali har bir kirish seansini IP-manzil, qurilma turi va vaqt tamg'asi bilan qayd etib boradi, bu esa xavfsizlik monitoringi va audit uchun asos yaratadi.

Natijalar

Taklif etilgan arxitektura asosida interfaol platformada autentifikatsiya va avtorizatsiya jarayonlari yagona OpenID + JWT + RBAC zanjiri orqali amalga oshirilishi ko'rsatildi. Foydalanuvchi tizimga kirishda avval email va parol orqali autentifikatsiyadan o'tadi, zarurat tug'ilganda esa SMS, email yoki autentifikator ilovasi orqali 2FA kodi tasdiqlanadi. Muvaffaqiyatli autentifikatsiyadan so'ng backend foydalanuvchining identifikatori va roli kodlangan JWT tokenni generatsiya qilib, mijoz tomoniga yuboradi. Keyingi so'rovlarda API Gateway ushbu tokenni HMAC-SHA256 imzo orqali verifikatsiya qiladi va payload ichidagi rol ma'lumotlariga tayangan holda RBAC qoidalarini qo'llaydi.

RBAC modelini ma'lumotlar bazasi darajasida implementatsiya qilishda "Admin", "Teacher", "Student" va "Guest" rollari uchun vakolatlar jadvali tuzilib, har bir rolning resurslarga kirish darajasi qat'iy chegaralandi. Admin tizim konfiguratsiyasi va barcha resurslarni boshqarish huquqiga ega, Teacher kurs yaratish, dars yuklash va test qo'yish funksiyalarini bajaradi, Student o'qish va test topshirish imkoniyatiga ega bo'ladi, Guest

esa faqat ochiq ma’lumotlarni ko‘rishi mumkin. Bunday taqsimot “least privilege” tamoyilini ta’minlab, har bir foydalanuvchiga faqat zarur minimal ruxsatlar berilishini kafolatlaydi. ERD diagrammasi foydalanuvchi–rol–ruxsat munosabatlarini grafik ko‘rinishda ifodalab, tizim modul va jadvallarining o‘zaro bog‘liqligini aniq ko‘rsatib beradi.

Muhokama

Natijalar shuni ko‘rsatadiki, parolga asoslangan autentifikatsiyani 2FA va JWT tokenlar bilan birgalikda qo‘llash interfaol o‘quv platformalarida axborot xavfsizligini sezilarli darajada oshiradi. Bir tomondan, ikki bosqichli autentifikatsiya hisoblarning buzilish ehtimolini kamaytirsa, ikkinchi tomondan, JWT asosidagi seans boshqaruvi server tarafida seans ma’lumotlarini saqlash zaruratini kamaytiradi va tizimni masshtablanuvchan qiladi. RBAC modelining ma’lumotlar bazasi darajasida formal tuzilishi foydalanuvchi amallarini qat’iy ruxsatlar matritsasi orqali boshqarishga imkon berib, tasodifiy yoki noto‘g‘ri konfiguratsiya natijasida ortiqcha vakolatlar berilishining oldini oladi.

Shu bilan birga, JWT tokenlarining o‘g‘irlanishi xavfi, token amal qilish muddati tugamaguncha ularni suiiste’mol qilish ehtimolini keltirib chiqarishi mumkin. Bu muammoni yumshatish uchun tokenning amal qilish muddatini qisqa belgilash, refresh tokenlar uchun alohida himoya siyosatini ishlab chiqish va Login_Logs bazasiga asoslangan faol monitoring mexanizmlarini qo‘llash zarur. Rollar va ruxsatlar soni ortgani sari RBAC modelini boshqarish murakkablashishi mumkin, shu sababli kelgusida atributlarga asoslangan kirish nazorati (ABAC) elementlarini integratsiya qilish maqsadga muvofiq hisoblanadi. Interfaol o‘quv platformalari kontekstida taklif etilgan yondashuv o‘qituvchi va talabalarga xavfsiz, boshqaruvi qulay va shaxsga moslashtirilgan muhit yaratishi bilan alohida ahamiyat kasb etadi.

Xulosa

Xulosa qilib aytganda, interfaol o‘quv platformalarida foydalanuvchini autentifikatsiya qilish va rollarga asoslangan kirish nazoratini tashkil etish uchun taklif etilgan OpenID + JWT + RBAC asosidagi uch qatlamli arxitektura texnik va tashkiliy jihatdan samarali yechimdir. Users, Roles, Permissions, User_Roles va Role_Permissions jadvallariga tayanuvchi ma’lumotlar bazasi modeli foydalanuvchi–rol–ruxsat munosabatlarini yagona struktura asosida boshqarish, “least privilege” tamoyilini tatbiq etish va himoyalangan API endpointlar uchun ruxsatlarni tekshirish imkonini beradi. Ushbu infratuzilma nafaqat ta’lim sohasida, balki moliyaviy xizmatlar, tibbiyot axborot tizimlari va korporativ platformalar kabi yuqori xavfsizlik talab etiladigan sohalarda ham qo‘llash uchun mos, masshtablanuvchan va integratsiyaga ochiq yechim sifatida baholanadi.

FOYDALANILGAN ADABIYOTLAR:

1. INTERFAOL PLATFORMADA FOYDALANUVCHI AUTENTIFIKATSIYASI VA ROLLARGA ASOSLANGAN KIRISH NAZORATI. ILM-FAN XABARNOMASI Volume 11, issue 1, Dekabr 2025

2. Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R. (2017). Guide to Attribute Based Access Control (ABAC): Definition and Considerations. NIST Special Publication 800-162.
3. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Assessment of Access Control Systems. NIST Special Publication 800-192.
4. OpenID Foundation. (2022). OpenID Connect Core 1.0 Specification. Available at: https://openid.net/specs/openid-connect-core-1_0.html
5. Jones, M., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT). IETF RFC 7519.
6. Jones, M., & Hardt, D. (2012). The OAuth 2.0 Authorization Framework. IETF RFC 6749.
7. OASIS Standard. (2013). eXtensible Access Control Markup Language (XACML) Version 3.0. Available at: https://docs.oasis-open.org/xacml/3.0/
8. Stallings, W. (2018). Cryptography and Network Security: Principles and Practice. Pearson.