Katta Tizimlarda Foydalanuvchilar Identifikatsiyasi va Autentifikatsiyasi: Algoritmlar va Texnologiyalar

Toshboltayev Faxriddin O‘rinboyevich.
FarDU Axborot texnologiyalari kafedrasi katta o‘qituvchisi
toshboltayevfaxriddin88@gmail.com
https://orcid.org/0000-0001-9661-3618
Qodiraliyev Jahonmurod Davronbek o‘g‘li
FarDU Axborot tizimlari va texnologiyalari
yo‘nalishi 2-kurs talabasi
jahonmurod37@gmail.com

Annotatsiya Ushbu maqolada katta hajmli axborot tizimlarida foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilishning dolzarb masalalari yoritilgan. Maqola zamonaviy algoritmlar va texnologiyalarni tahlil qilishga, jumladan, parollarga asoslangan, ko‘p faktorli, biometrik va tokenlarga asoslangan usullarning xususiyatlari va samaradorligiga qaratilgan. Amaliy qismda ushbu mexanizmlarni joriy etish orqali tizimning himoyalanganlik darajasini oshirishga va ruxsatsiz kirishlarning oldini olishga qaratilgan amaliy tavsiyalar berilgan.

Kalit so‘zlar: Identifikatsiya, autentifikatsiya, ko‘p faktorli autentifikatsiya (MFA), biometriya, parol, xavfsizlik, token.

Аннотация. В данной статье рассматриваются актуальные вопросы идентификации и аутентификации пользователей в крупномасштабных информационных системах. Основное внимание уделяется анализу современных алгоритмов и технологий, включая особенности и эффективность парольных, многофакторных, биометрических и токен-основанных методов. В практической части представлены рекомендации, направленные на повышение уровня защиты системы и предотвращение несанкционированного доступа посредством внедрения этих механизмов.

Ключевые слова: Идентификация, аутентификация, многофакторная аутентификация (MFA), биометрия, пароль, безопасность, токен.

Abstract. This article addresses the pressing issues of user identification and authentication in large-scale information systems. The focus is on analyzing contemporary algorithms and technologies, including the features and effectiveness of password-based, multi-factor, biometric, and token-based methods. The practical

section provides recommendations aimed at enhancing the system's security level and preventing unauthorized access through the implementation of these mechanisms.

Keywords: Identification, Authentication, Multi-Factor Authentication (MFA), Biometrics, Password, Security, Token.

KIRISH

Zamonaviy raqamli dunyoda, katta korporativ tarmoqlardan tortib, bulutli platformalargacha bo‘lgan katta tizimlarda ma’lumotlar xavfsizligini ta’minlash eng muhim vazifalardan biridir. Ushbu xavfsizlikning asosi — bu tizimga kiruvchi har bir foydalanuvchining shaxsini ishonchli tarzda aniqlash, ya’ni identifikatsiya (kim ekanligini e’lon qilish) va autentifikatsiya (e’lon qilingan shaxsni tasdiqlash) jarayonlaridir. Ushbu maqola katta tizimlarda qo‘llaniladigan ushbu jarayonlarning samaradorligini oshirishga qaratilgan algoritmlar va texnologiyalarni o‘rganishga bag‘ishlangan.

Asosiy qism

Identifikatsiya va Autentifikatsiya Tushunchalari

1. Identifikatsiya: Foydalanuvchining tizimga o‘zining noyob nomini (login, ID) yoki boshqa shaxsiy belgisini taqdim etishi. Bu faqat e’lon qilish.

Autentifikatsiya: Foydalanuvchining e’lon qilingan shaxs ekanligini isbotlash jarayoni. Bu odatda quyidagi uch usuldan biri orqali amalga oshiriladi:

- ❖ Bilgan narsa (Masalan, parol, PIN-kod). bo‘lgan
- ❖ Ega narsa (Masalan, mobil telefon, xavfsizlik tokeni).
- ❖ O‘ziga xos narsa (Masalan, barmoq izi, yuz shakli, ovoz - biometriya).

2. Autentifikatsiya Algoritmlari va Texnologiyalari

Katta tizimlarda xavfsizlik talablariga qarab turli xil autentifikatsiya mexanizmlari qo‘llaniladi:

Parollarga asoslangan autentifikatsiya (Password-Based Authentication):

Algoritmlar: Kriptografik hash funksiyalari (masalan, SHA-256, bcrypt, scrypt) parollarni xavfsiz saqlash uchun ishlatiladi. Parol tekshirishda hash qiymatlari solishtiriladi, asl parol bazada saqlanmaydi.

Texnologiyalar: Salt (tuz) qo‘shish (parolni hash qilishdan oldin unga tasodifiy satr qo‘shish) va pepper (qalampir) qo‘shish (tizim miqyosida qo‘shiladigan yashirin qiymat) usullari kuchli himoyani ta’minlaydi. 2.2. Ko‘p faktorli autentifikatsiya (MFA / 2FA):

Bu foydalanuvchidan kamida ikkita turli xil autentifikatsiya faktorini (masalan, parol va SMS-kod) taqdim etishni talab qiladi.

Texnologiyalar: TOTP (Time-based One-Time Password - vaqtga asoslangan bir martalik parol) va HOTP (HMAC-based One-Time Password) algoritmlari eng keng tarqalgan bo‘lib, Google Authenticator, Authy kabi ilovalarda qo‘llaniladi.

Biometrik autentifikatsiya (Biometric Authentication):

Foydalanuvchining biologik xususiyatlari (barmoq izi, yuz, ko‘zning rangdor pardasi) asosida ishlaydi.

Algoritmlar: Naqshlarni aniqlash (Pattern Recognition) va Xususiyatlarni ajratish (Feature Extraction) algoritmlari skanerlangan biometrik ma’lumotni shablon (template)ga aylantirish uchun ishlatiladi. Shablonlar kriptografik usulda himoyalanib saqlanadi.

Tokenlarga asoslangan autentifikatsiya:

Texnologiyalar: OAuth 2.0 (avtorizatsiya uchun) va OpenID Connect (identifikatsiya uchun) kabi standartlar, shuningdek, JWT (JSON Web Tokens) kabi kriptografik tokenlar zamonaviy veb-tizimlar va API larda keng qo‘llaniladi.

3. Katta Tizimlarda Qo‘llashning O‘ziga Xosliklari

Katta tizimlarda autentifikatsiya mexanizmlari quyidagi talablarga javob berishi kerak:

- ❖ Masshtablanuvchanlik: Bir vaqtning o‘zida minglab foydalanuvchilarni ishonchli autentifikatsiya qilish imkoniyati.
- ❖ Markazlashgan boshqaruv: SSO (Single Sign-On - Yagona kirish) mexanizmi orqali bitta identifikatsiya bilan ko‘plab xizmatlarga kirish imkoniyatini berish. SAML (Security Assertion Markup Language) kabi protokollar SSO ni ta’minlashda muhim rol o‘ynaydi.
- ❖ Yuqori ishonchlilik: Autentifikatsiya xizmatlarining doimiy ishlashi ta’minlanishi.

XULOSA

Katta tizimlarda foydalanuvchilarning identifikatsiyasi va autentifikatsiyasi tizim xavfsizligini ta’minlashning eng muhim bosqichidir. Faqatgina kuchli parollarga tayanish zamonaviy xatarlarga qarshi yetarli emas. Shuning uchun, ko‘p faktorli autentifikatsiya (MFA) va ilg‘or biometrik texnologiyalarni joriy etish orqali tizimdagi ma’lumotlar himoyalanadi va ruxsatsiz kirishlarning oldi olinadi. Hashlash

algoritmlarini (bcrypt, scrypt) to‘g‘ri qo‘llash hamda SSO yechimlarini (SAML, OpenID Connect) markazlashtirilgan holda boshqarish tizimning barqaror va xavfsiz ishlashini ta’minlaydi.

Foydalanilgan adabiyotlar

1. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization.
3. National Institute of Standards and Technology (NIST) Special Publication 800-63-3. Digital Identity Guidelines. NIST, U.S. Department of Commerce.
4. Jøsang, A., Vestre, J., & Wergeland, R. (2012). Authentication Technologies and Protocols. University of Oslo.