BIOMETRIKA VA AXBOROT XAVFSIZLIGI

Nurniyazov Arman Arzubay uli
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
1-bosqich magistranti

Annotatsiya: Maqolada biz biometrik autentifikatsiyasi nima ekanligini, u qayerda qo‘llanilishini, axborot xavfsizligi kontekstida uning afzalliklari va kamchiliklarini ko‘rib chiqamiz va biometrikadan foydalanish mexanizmlarining qaysi biri ishonchli bo‘lishi mumkinligini tushunishga harakat qilamiz.

Kalit so‘zlar: biometrik tizimlar, shaxsiy biometrik ma’lumotlar, identifikatsiya, autentifikatsiya, avtorizatsiya, axborot xavfsizligi.

Biometrik autentifikatsiya kompaniyalar uchun ham, oddiy foydalanuvchilar uchun ham axborotni himoya qilishning afzal usuliga aylanib bormoqda. Yaqin vaqtlargacha barmoq izi yoki yuz orqali biror narsaga kirish ilmiy fantastikaning bir toifasiga o‘xshardi. Bugungi kunda ko‘pchilik uchun smartfonni shu tarzda ochish odat tusiga kirgan.

Biometrika identifikatsiya, autentifikatsiya va avtorizatsiya uchun ishlatiladi - bular bir-biri bilan chambarchas bog‘liq bo‘lgan uchta ketma-ket jarayondir. Identifikatsiya qilishda biz tizimni noyob namuna - identifikator bilan taqdim etamiz, shundan so‘ng tizim ushbu namunani ma’lumotlar bazasida saqlangan shablon bilan taqqoslaydi - autentifikatsiya sodir bo‘ladi. Agar taqdim etilgan namuna shablonga mos keladigan bo‘lsa, foydalanuvchiga ma’lum huquqlar to‘plamiga kirish huquqi beriladi - avtorizatsiya sodir bo‘ladi.

Biometrik autentifikatsiya – bu shaxsning o‘ziga xos biologik xususiyatlarini ko‘rsatishga asoslangan autentifikatsiya usuli: barmoq izi, yuz geometriyasi, kaft shakli. Biometrik xarakteristikalar, shuningdek, quloqning shakli, tana hidi, yurak

urishi, qo‘llardagi tomirlarning naqshlari, DNK - bularning barchasi ma’lum bir shaxsning noyob biometrik identifikatorlari hisoblanadi. Har bir insonning xatti-harakati va harakatlarining o‘ziga xos xususiyatlariga asoslanadigan xulq-atvor biometrikasi ham mavjud. Uning misollari – yurish, ovoz, qo‘l yozuvi, shu jumladan klaviatura qo‘l yozuvi (terish tezligi va dinamikasi, xatolik darajasi, ma’lum tugmachalardan foydalanish).

Amalda biometrik autentifikatsiya usullari ko‘plab sohalarda, jumladan, harbiy, huquqni muhofaza qilish, moliya va elektron tijoratda samarali qo‘llaniladi.

Afzalliklar:

- Birinchidan, bu qulay. Foydalanuvchiga murakkab parollarni eslab qolishi shart emas. Barmoqni, ko‘zni, quloqni yoki yuzni ko‘rsatish yoki ovoz chiqarish kifoya va kirishga ruxsat beriladi. Biometrik ma’lumotlar har doim siz bilan, uni yo‘qotish yoki unutish mumkin emas.
- Ikkinchidan, biometrik ma’lumotlarni o‘g‘irlash kalit yoki parol kabi oson emas. Bir qarashda, biometrik autentifikatsiya zaif parollar muammosini hal qiladi, statistik ma'lumotlarga ko‘ra, 80% hollarda akkauntni parol orqali buzish holatlari bo‘ladi.
- Uchinchidan, biometrik autentifikatsiyadan korporativ maqsadlarda foydalanishda autentifikatsiya tizimini saqlash xarajatlari kamayadi, parollarni muntazam ravishda o‘zgartirish, unutilgan va yo‘qolgan parollarni qayta tiklashga pul va vaqt sarflashning hojati yo‘q.
- To‘rtinchidan, biometrik autentifikatsiyadan foydalanish masofaviy xakerliklarni murakkablashtiradi. Parolni bilsa ham, biometrik ma’lumotlar qo‘shimcha identifikator sifatida ishlaydigan ikki faktorli autentifikatsiya sozlangan bo‘lsa, tajovuzkorlar maqsadli tizim yoki qurilmaga kira olmaydi.

Kamchiliklari:

- Biometrik “spoofing”. Spoofing - bu soxta yoki nusxalangan ma’lumotlardan, bu holda biometrik ma’lumotlardan foydalangan holda xavfsizlik tizimini aldash amaliyotidir. Misol uchun, barmoq izini ob’ektdan suratga olish va nusxa ko‘chirish

mumkin. Soxta barmoq izi mobil qurilma yoki to‘lov tizimini blokdan chiqarish uchun ishlatilishi mumkin, bu esa tajovuzkorlarga foydalanuvchi ma’lumotlari va bank hisobiga kirish imkonini beradi.

- Xatolik. Qonuniy foydalanuvchiga kirishni rad etish yoki ruxsatsiz shaxsga noto‘g‘ri ruxsat berish. Masalan, egizak akasi yoki singlisi bo‘lganlar uchun yuzni aniqlash usuli tavsiya etilmaydi. Biometrik usulda qanchalik ishonchli bo‘lmasin, har doim noto‘g‘ri salbiy va noto‘g‘ri ijobiy javob berish ehtimoli mavjud. Masalan, sizning ovozli identifikatoringiz ham 100% xavfsiz emas. Ma’lumki, sun’iy intellekt va mashinani o‘rganishga asoslangan deepfakes (neyron tarmoqlar tomonidan yaratilgan soxta video yoki audio ma’lumotlar) ovozlarni ishonchli tarzda taqlid qilishi mumkin.
- Biometrik ma’lumotlar kompaniya serverlarida saqlanadi. Ushbu ma’lumotlarga ega bo‘lgan ma’lumotlar bazalari xavfsiz himoyalanganligi va uchinchi shaxslarga o‘tkazilmasligiga kafolat yo‘q. Agar tajovuzkorlar bunday ma’lumotlar bazasiga kirish huquqiga ega bo‘lsalar, ular shaxsiy ma’lumotlar va mablag‘larni o‘g‘irlash uchun buzilgan hisoblardan foydalanishlari mumkin.

Biometrik autentifikatsiya sohasi istiqbolli va jadal rivojlanmoqda, bu sohadagi tadqiqot va ishlanmalar soni yildan-yilga ortib bormoqda. Biroq, bu usullar mukammal emas va har doim xatolik ehtimoli mavjud. Maxfiy ma’lumotlaringiz va pullaringizni himoya qilish uchun biometrikadan foydalanishga qaror qilishdan oldin, ijobiy va salbiy tomonlarini diqqat bilan ko‘rib chiqishga arziydi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Мировой рынок биометрических систем, 2015–2022 гг. – Электрон. текстовые дан. – Режим доступа: http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618 (дата обращения: 23.10.2019).

2. Сабанов, А. Г. Сравнительный анализ ме-тодов биометрической идентификации личности /А. Г. Сабанов, С. Г. Смолина. – М. : Труды ИСА РАН, 2016. – Т. 66. – С. 11–20.