

SUN'IY INTELLEKT ASOSIDA BIOMETRIK AUTENTIFIKATSIYA TIZIMLARINING XAVFSIZLIGI

Imamaliyev Aybek Turapbayevich

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti dotsenti, PhD

G'ulomova Ko'hinur Murod qizi

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Usmonov Faxriddin Sharofiddin o'g'li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Mazkur maqolada sun'iy intellekt asosida biometrik autentifikatsiya tizimlarining xavfsizligi masalalari tahlil qilinadi. Hozirgi kunda biometrik autentifikatsiya texnologiyalari axborot tizimlarida keng qo'llanilmoqda. Sun'iy intellekt ushbu tizimlarning aniqligi va tezligini oshirishga xizmat qilsa-da, ularning xavfsizligi bilan bog'liq bir qator muammolar ham mavjud. Maqolada biometrik tizimlarga nisbatan amalga oshiriladigan hujumlar, jumladan spufing, deepfake va ma'lumotlar sizib chiqishi kabi tahdidlar ko'rib chiqiladi. Shuningdek, ushbu tizimlarni himoya qilish usullari va zamonaviy xavfsizlik mexanizmlari tahlil qilinadi.

Kalit so'zlar: Biometrik autentifikatsiya, sun'iy intellekt, yuzni aniqlash, barmoq izi, deepfake, spufing, kiberxavfsizlik, autentifikatsiya tizimlari, AI xavfsizligi.

Kirish

Axborot texnologiyalarining jadal rivojlanishi natijasida foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash usullari ham tubdan o'zgarib bormoqda. An'anaviy autentifikatsiya usullari, masalan, parol va PIN-kodlarga asoslangan tizimlar o'zining zaif tomonlari sababli tobora samarasiz bo'lib bormoqda. Ayniqsa, parollarni unutish, ularni boshqalarga berish yoki to'liq ajratib bajariladigan hujumlar orqali buzish ehtimoli yuqori bo'lgani sababli, zamonaviy xavfsizlik tizimlari biometrik autentifikatsiya usullariga tobora ko'proq murojaat qilmoqda.

Biometrik autentifikatsiya – bu foydalanuvchini uning jismoniy yoki xulq-atvoriga xos xususiyatlari asosida aniqlash usulidir. Ushbu texnologiyaga yuzni aniqlash, barmoq izi, ovoz, retina yoki iris skanerlash kabi usullar kiradi. Biometrik tizimlarning asosiy afzalligi shundaki, ular foydalanuvchiga bog'liq bo'lgan noyob xususiyatlardan foydalanadi va shu sababli ularni qalbakilashtirish nisbatan murakkab hisoblanadi.

So'nggi yillarda sun'iy intellekt, xususan, mashinaviy o'rganish va chuqur o'rganish algoritmlarining rivojlanishi biometrik tizimlarning samaradorligini sezilarli darajada oshirdi. AI yordamida yuzni aniqlash tizimlari inson yuzidagi murakkab naqshlarni aniqlay oladi, ovozni aniqlash tizimlari esa nutqdagi o'ziga xos xususiyatlarni ajratib ko'rsatadi. Bu esa autentifikatsiya jarayonini yanada tez va aniq ishlashiga imkon beradi. Biroq, sun'iy intellektning biometrik autentifikatsiya tizimlariga joriy etilishi bilan bir qatorda yangi xavfsizlik tahdidlari ham yuzaga kelmoqda. Masalan, deepfake texnologiyalari yordamida foydalanuvchining yuzini yoki ovozini soxtalashtirish mumkin. Bu esa yuzni aniqlash tizimlarini aldash imkonini beradi. Shuningdek, spufing hujumlari orqali biometrik tizimlariga soxta ma'lumotlar taqdim etilishi mumkin.

Bundan tashqari, biometrik ma'lumotlar o'zining maxfiyligi bilan ajralib turadi. Agar parol o'g'irlangan bo'lsa, uni o'zgartirish mumkin, biroq biometrik ma'lumotlarni (masalan, barmoq izi yoki yuz tasviri) o'zgartirib bo'lmaydi. Shu sababli, biometrik ma'lumotlarning sizib chiqishi juda katta xavf tug'diradi. Bu esa ushbu tizimlarda ma'lumotlarni himoya qilishni yanada muhim vazifaga aylantiradi.

Zamonaviy biometrik tizimlarda AI yordamida xavfsizlikni oshirishga qaratilgan turli mexanizmlar joriy etilmoqda. Masalan, triklikka tekshirish (liveness detection) texnologiyasi yordamida tizim real insonni va soxta tasvirni farqlay oladi. Bundan tashqari, ko'p faktorli autentifikatsiya tizimlari (biometrik + parol yoki token) orqali xavfsizlik darajasi yanada oshiriladi.

Shu bilan birga, biometrik autentifikatsiya tizimlarining ishlashida xatolik ehtimoli ham mavjud. Ba'zi hollarda tizim haqiqiy foydalanuvchini tanimasligi yoki aksincha, begona shaxsni qabul qilishi mumkin. Bu esa tizimning ishonchliligiga ta'sir ko'rsatadi.

Mazkur maqolada sun'iy intellekt asosida biometrik autentifikatsiya tizimlarining xavfsizlik muammolari, ularga nisbatan amalga oshiriladigan hujumlar va ushbu tizimlarni himoya qilish usullari keng yoritiladi. Shuningdek, zamonaviy texnologiyalar yordamida biometrik tizimlarning xavfsizligini oshirish imkoniyatlari ham tahlil qilinadi.

2. Biometrik autentifikatsiya turlari

Biometrik autentifikatsiya tizimlari foydalanuvchini uning o'ziga xos biologik va xulq-atvor xususiyatlari orqali aniqlashga asoslanadi. Ushbu tizimlar zamonaviy axborot xavfsizligida muhim o'rin egallab, an'anaviy parol va PIN-kodlarga nisbatan ancha ishonchli hisoblanadi. Biometrik autentifikatsiya ikki asosiy turga bo'linadi: fiziologik va xulq-atvor biometrikasi.

Fiziologik biometrika insonning jismoniy xususiyatlariga asoslanadi. Bu turga barmoq izi, yuzni aniqlash, iris yoki retinani skanerlash kabi usullar kiradi. Masalan, barmoq izi orqali autentifikatsiya qilish bugungi kunda eng keng tarqalgan usullardan biri bo'lib, ko'plab mobil qurilmalarda qo'llaniladi. Yuzni aniqlash esa sun'iy intellekt yordamida ishlaydi va foydalanuvchining yuzidagi noyob belgilarni tahlil qilish orqali uni aniqlaydi. Ushbu usullar yuqori aniqlik va qulaylikni ta'minlaydi, biroq ayrim hollarda soxtalashtirish xavfi ham mavjud.

Xulq-atvor biometrikasi esa foydalanuvchining harakatlari va odatlariga asoslanadi. Masalan, klaviatura bosish tezligi, ovoz ohangi yoki imzo qo'yish uslubi orqali foydalanuvchini aniqlash mumkin. Bu tur biometrika ko'pincha qo'shimcha xavfsizlik chorasi sifatida ishlatiladi. Uning afzalligi shundaki, foydalanuvchi bu jarayonni sezmasligi mumkin, biroq aniqlik darajasi fiziologik biometrikaga nisbatan pastroq bo'lishi mumkin.

3. Biometrik autentifikatsiya tizimlarida xavfsizlik tahdidlari

Biometrik autentifikatsiya tizimlari yuqori darajada ishonchli hisoblanganiga qaramay, ular ham turli xil kiberhujumlarga duch keladi. Ushbu tahdidlar tizimning ishonchliligini pasaytirishi va foydalanuvchi ma'lumotlarining xavfsizligiga jiddiy zarar yetkazishi mumkin.

Eng keng tarqalgan tahdidlardan biri bu spufing hujumlaridir. Bu hujumda tajovuzkor tizimni aldash uchun soxta biometrik ma'lumotlardan foydalanadi. Masalan, silikon barmoq izi yoki fotosurat yordamida yuzni aniqlash tizimini aldash mumkin. Bu kabi hujumlar biometrik tizimlarning zaif tomonlarini ochib beradi.

Yana bir muhim tahdid – bu deepfake texnologiyalari hisoblanadi. Sun'iy intellekt yordamida inson yuzini yoki ovozini realga juda o'xshash tarzda yaratish mumkin. Bu esa biometrik autentifikatsiya tizimlarini aldash imkonini beradi. Ayniqsa, ovoz va yuz orqali autentifikatsiya tizimlari uchun bu katta xavf tug'diradi.

Shuningdek, biometrik ma'lumotlarning sizib chiqishi ham katta muammo hisoblanadi. Agar parol o'g'irlangan bo'lsa, uni o'zgartirish mumkin, biroq biometrik ma'lumotlarni almashtirib bo'lmaydi. Shu sababli, bunday ma'lumotlarning himoyasi alohida e'tibor talab qiladi. Bundan tashqari, replay attack deb ataluvchi hujum turi ham mavjud bo'lib, bunda oldin yozib

oligan biometrik ma'lumot qayta ishlatilib, tizimga noqonuniy kirish amalga oshiriladi. Bu esa tizimni yanada murakkab himoya mexanizmlariga muhtoj qiladi.

4. Biometrik autentifikatsiya tizimlarini himoya qilish usullari

Biometrik autentifikatsiya tizimlarining xavfsizligini ta'minlash uchun zamonaviy texnologiyalar va kompleks yondashuvlar zarur. Bunda bir nechta muhim himoya usullari mavjud bo'lib, ular tizimni turli xil hujumlardan himoya qilishga yordam beradi.

Birinchi navbatda, liveness detection texnologiyasi muhim ahamiyatga ega. Ushbu texnologiya foydalanuvchining haqiqiy inson ekanligini aniqlashga yordam beradi. Masalan, tizim foydalanuvchidan ko'z qimirlatishni yoki boshini harakatlantirishni talab qilishi mumkin. Bu esa fotosurat yoki video orqali tizimni aldashning oldini oladi.

Ikkinchi muhim usul – ko'p faktorli autentifikatsiya hisoblanadi. Bu usulda biometrik autentifikatsiya boshqa usullar bilan birgalikda qo'llaniladi. Masalan, yuzni aniqlash bilan birga parol yoki SMS koddan foydalanish tizim xavfsizligini sezilarli darajada oshiradi.

Shuningdek, sun'iy intellekt asosida monitoring tizimlari ham muhim rol o'ynaydi. Bunday tizimlar foydalanuvchi xatti-harakatlarini tahlil qilib, g'ayrioddiy faoliyatni aniqlaydi va avtomatik ravishda xavf haqida ogohlantiradi.

Bundan tashqari, biometrik ma'lumotlarni shifrlash ham juda muhim hisoblanadi. Zamonaviy kriptografik algoritmlar yordamida ma'lumotlar himoyalangani va ular o'g'irlangan taqdirda ham foydalanish qiyinlashadi.

Amaliy jihatdan qaraydigan bo'lsak, zamonaviy smartfonlarda yuzni aniqlash tizimlari liveness detection bilan birgalikda ishlaydi. Bu esa oddiy fotosurat orqali tizimni aldash imkoniyatini deyarli yo'q qiladi. Shuningdek, bank tizimlarida biometrik autentifikatsiya SMS kod bilan birga qo'llanilib, xavfsizlik darajasi yanada oshiriladi.

Xulosa

Mazkur maqolada sun'iy intellekt asosida biometrik autentifikatsiya tizimlarining xavfsizligi masalalari yoritildi. Biometrik tizimlar zamonaviy autentifikatsiya usullarining eng ilg'or ko'rinishlaridan biri bo'lib, foydalanuvchilarga yuqori darajada qulaylik va aniqlikni ta'minlaydi. Shu bilan birga, ular spufing, deepfake va ma'lumotlar sizishi kabi tahdidlarga duch keladi.

Tahlillar shuni ko'rsatadiki, biometrik tizimlarning xavfsizligini ta'minlash uchun liveness detection, ko'p faktorli autentifikatsiya, sun'iy intellekt asosida monitoring va ma'lumotlarni shifrlash kabi usullar samarali hisoblanadi. Ushbu yondashuvlar orqali tizimni yanada ishonchli qilish mumkin.

Xulosa qilib aytganda, biometrik autentifikatsiya tizimlari kelajakda yanada rivojlanadi va keng qo'llaniladi. Shu sababli, ularning xavfsizligini ta'minlash va yangi tahdidlarga qarshi kurashish dolzarb masala bo'lib qoladi.

Foydalanilgan adabiyotlar

1. Jain A. K. Biometric recognition: overview and recent advances //Iberoamerican Congress on Pattern Recognition. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2007. – C. 13-19.
2. Goodfellow I. et al. Deep learning. – Cambridge : MIT press, 2016. – T. 1. – №. 2. – C. 1-800.
3. Grassi P. A., Garcia M. E., Fenton J. L. Draft nist special publication 800-63-3 digital identity guidelines //National Institute of Standards and Technology, Los Altos, CA. – 2017.
4. Kaspersky – Biometric Security. Veb sayt: <https://www.kaspersky.com/resource-center/definitions/biometrics> (Murojaat vaqti: 10.04.2026y)
5. IBM Security Reports. Veb sayt: <https://www.ibm.com/reports/threat-intelligence> (Murojaat vaqti: 10.04.2026y)