Biometrik ma‘lumotlarni shifrlash va saqlash: Face ID tizimlarida ma’lumotlar xavfsizligi

Buxoro davlat universiteti
Fizika-matematika va axborot texnologiyalari fakulteti magistranti
No‘monjonova Sitora Muzaffar qizi
sitoranomonjonova617@gmail.com

Annotatsiya. Ushbu maqolada Face ID tizimlarida biometrik ma'lumotlarni shifrlash va saqlash jarayonlari, shuningdek, ma’lumotlar xavfsizligini ta’minlash usullari tahlil qilinadi. Shuningdek, biometrik ma’lumotlarning noyob xususiyatlari, ularni shifrlashda qo’llaniladigan zamonaviy kriptografik usullar va xavfsizlikka qarshi tahdidlar o‘rganilgan.

Kalit so'zlar: biometrik autentifikatsiya, Face ID, ma'lumotlar shifrlash, biometrik template, xavfsizlik, 3D skanerlash, **hash funksiyalar** ma'lumotlar himoyasi.

Kirish

Zamonaviy raqamli dunyo sharoitida biometrik autentifikatsiya tizimlari, xususan, Face ID texnologiyasi keng tarqalgan. Biometrik autentifikatsiya tizimlari hozirgi kunda axborot xavfsizligi sohasida muhim o‘rin tutadi. Face ID texnologiyasi, jumladan, yuz tanish asosidagi autentifikatsiya tizimlari mobil qurilmalar va boshqa raqamli platformalarda keng qo‘llanilmoqda. Biometrik ma’lumotlarning noyob va o‘zgarmas tabiati ularni maxfiy saqlash va ishonchli shifrlash zaruratini yuzaga keltirmoqda.

O‘zbekiston Respublikasi Prezidentining 2024-yil 24-maydagi “Ma’muriy islohotlar doirasida adliya organlari va muassasalarining mas’uliyatini yanada oshirish hamda ixcham boshqaruv tizimini shakllantirish to‘g‘risida”gi farmoni bilan adliya organlarini xalqqa yanada yaqinlashtirish, ularning faoliyatini takomillashtirish va boshqaruv tizimini optimallashtirishga qaratilgan bir qator chora-tadbirlar belgilangan[1].

[1] O‘zbekiston Respublikasi Prezidentining 2024-yil 24-maydagi “Ma’muriy islohotlar doirasida adliya organlari va muassasalarining mas’uliyatini yanada oshirish hamda ixcham boshqaruv tizimini shakllantirish to‘g‘risida”gi farmonidan

Ushbu farmon orqali davlat xizmatlarini ko‘rsatishda Face-ID texnologiyasi joriy etilishi, shuningdek, “Fuqaro – mahalla – adliya” tizimini joriy etish ko‘zda tutilgan.

Face-ID tizimi orqali davlat xizmatlarini ko‘rsatishda shaxsni aniqlashning xavfsiz usuli joriy qilindi, bu esa fuqarolarga yanada qulaylik yaratdi.

Biometrik ma’lumotlar an’anaviy parollar yoki PIN kodlardan farqli o‘laroq, insonning biologik xususiyatlariga asoslangan bo‘ladi va ularni o‘zgartirish yoki tiklash imkoni yo‘q. Shuningdek, ushbu ma’lumotlarning buzilishi yoki noto‘g’ri foydalanilishi xavfsizlik tizimida jiddiy muammolarni keltirib chiqarishi mumkin. Face ID tizimlarida yuz tasvirining matematik tasviri maxfiylik va xavfsizlik nuqtai nazaridan alohida e'tibor talab qiladi. Shu sababli, ushbu tasvirlar xotirada biometrik template shaklida saqlanadi.

Zamonaviy Face ID tizimlari infraqizil nurlar, 3D skanerlash va chuqur o‘rganish algoritmlaridan foydalanib, yuqori aniqlik darajasiga erishmoqda. Biroq, ushbu texnologiyalarning rivojlanishi bilan birga yangi xavfsizlik muammolari ham paydo bo‘lmoqda. Shuning uchun biometrik ma’lumotlarni samarali shifrlash va himoya qilish usullarini o‘rganish hozirda ushbu soha vakillarining eng dolzarb vazifa hisoblanadi.

Asosiy qism

Face ID tizimi bir necha asosiy komponentlardan iborat. Ularning har biri ma’lumotlar xavfsizligida muhim rol o‘ynaydi. **Biometrik sensor moduli:** TrueDepth kamerasi infraqizil projektorlar va kameralar yordamida yuzning 3D xaritasini yaratadi. Bu jarayonda 30,000 dan ortiq nuqta skanerlanib, yuzning matematik modeli hosil qilinadi. **Ma’lumotlarni qayta ishlash blokida esa o**lingan biometrik ma’lumotlar maxsus algoritmlar yordamida matematik hash qiymatlar to’plami bo‘lgan biometrik templatega aylantiriladi. Shuningdek, bu template asl tasvir hisoblanmaydi. Biometrik templatelar Secure Enclave yoki shunga o‘xshash maxfiy muhitda shifrlangan holda saqlanadi. Bu muhit operatsion tizimdan ajratilgan va to‘g’ridan-to‘g’ri kirish imkoni yo‘q.

Hozirgi kunda Face ID tizimlarida eng ko‘p qo‘llaniladigan asosiy shifrlash texnologiyalari quyidagilar:

AES (Advanced Encryption Standard) shifrlash: Biometrik templatelar odatda AES-256 shifrlash algoritmi yordamida himoyalanadi. Bu algoritm hozirgi kunda eng ishonchli simmetrik shifrlash usullaridan biri hisoblanadi.

Elliptik egri kriptografiya (ECC): Kalitlar almashinuvi va raqamli imzo qo‘yish uchun ushbu algoritmlar qo‘llaniladi. Bu usul orqali kichik kalit o‘lchamlari bilan yuqori xavfsizlik darajasi ta’minlanadi.

Hash funksiyalar: SHA-256 va SHA-3 kabi kriptografik hash funksiyalar odatda biometrik ma’lumotlarning yaxlitligini tekshirish uchun ishlatiladi.

Homomorph shifrlash: Ilg’or Face ID tizimlari uchun homomorph shifrlash texnologiyasidan foydalanish juda qulay. Chunki bunda ushbu shifrlangan ma’lumotlar ustida to‘g’ridan-to‘g’ri hisob-kitoblar olib borish imkoni mavjud.

Biometrik template hosil qilish ham murakkab jarayon hisoblanadi. Bunda avvalo, yuz tasviridan asosiy geometrik xususiyatlar (ko‘zlar orasidagi masofa, burun shakli, og’iz konturi) ajratiladi. Turli sharoitlarda olingan tasvirlarni bir xil formatga keltirish uchun yorug’lik, burchak va o‘lchamlar bo‘yicha normallashtirish amalga oshiriladi. Ajratilgan xususiyatlar asosida matematik vector yoki hash qiymatlari to‘plami yaratiladi. Biroq bu template asl tasvirni tiklash imkonini bermaydi. Ba’zi tizimlar Fuzzy Vault kriptografik protokolidan foydalanib, biometrik templateni himoya qiladi. Bu usulda templatega shovqinli ma’lumotlar qo‘shish orqali asl ma’lumotlarni yashirishadi.

Zamonaviy texnologiyalar rivojlanganligi sari ularga bo‘lgan tahdidlar va hujum usullari ham rivojlanib, ko‘payib bormoqda. Masalan, **template hujumlari-b**uzg’unchilar biometrik templateni o‘g’irlash orqali tizimga kirish huquqini olishga harakat qilishi mumkin. **Presentation hujumlari-fo**to, video yoki 3D modellar yordamida tizimni aldashga urinish. **Side-channel hujumlari-q**urilmaning energiya iste’moli yoki elektromagnit signallari orqali ma’lumot olishi. **Template reconstruction hujumlari-b**a’zi tadqiqotlar ko‘rsatishicha, matematik templatelar asosida asl yuz tasvirini taxminan tiklash mumkin.

Raqamli dunyoning tez rivojlanishi bilan biometrik autentifikatsiya texnologiyalari an’anaviy parol va PIN-kod sistemalarini siqib chiqarmoqda. Face ID texnologiyasi, ayniqsa, mobil qurilmalar va korporativ xavfsizlik tizimlarida keng qo‘llanilmoqda. Biroq, biometrik ma’lumotlarning noyob va o‘zgarmas tabiati ularni

alohida himoya choralarini talab qiluvchi strategik aktivlarga aylantiradi. Zamonaviy Face ID tizimlarida Apple kompaniyasining Secure Enclave texnologiyasidan tortib to cloud-based biometrik xizmatlarining murakkab arxitekturasigacha turli yondashuvlar mavjud. Har bir yondashuv o‘zining afzalliklari va cheklovlariga ega bo‘lib, ma’lum sharoitlarda qo‘llaniladi.

An’anaviy autentifikatsiya usullaridan farqli o‘laroq, biometrik ma’lumotlar buzilganda ularni qayta tiklash yoki o’zgartirish imkonsizdir. Agar foydalanuvchining paroli buzilsa, u yangi parol o‘rnatishi mumkin, ammo biometrik ma’lumotlar bir marta buzilganda, bu ma’lumotlar butun hayot davomida xavfsiz bo‘lmay qoladi. Shuning uchun biometrik ma‘lumotlarni himoyalash an’anaviy ma’lumotlar xavfsizligidan ancha murakkab masaladir.

Face ID tizimlarida ma’lumotlar xavfsizligi bir necha asosiy yo‘nalishni o‘z ichiga oladi: biometrik shablonlarni xavfsiz yaratish, ularni shifrlangan holda saqlash, himoyalangan kanallar orqali uzatish va maxfiylikni saqlagan holda autentifikatsiya amalga oshirish. Har bir bosqichda turli xil kriptografik va texnik yechimlar qo‘llaniladi.

Biometrik ma’lumotlarning noyob tabiati ularni himoyalashda an'anaviy ma'lumotlar xavfsizligidan butunlay boshqacha yondashuvni talab qiladi. Buzilgan parolni o‘zgartirish mumkin, ammo biometrik ma’lumotlar bir marta buzilganda bu zararni qayta tiklab bo’lmaydi.

Zamonaviy kriptografik usullar - AES-256, elliptik egri kriptografiyasi va hash funksiyalari - biometrik ma’lumotlarni samarali himoyalash uchun yetarli, ammo ularni to‘g’ri qo‘llash muhim ahamiyatga ega. Hardware Security Modules va Secure Enclave kabi apparatli yechimlar eng yuqori darajadagi xavfsizlikni ta’minlaydi.

Template Protection texnikalari - cancelable biometrics, homomorphic encryption va secure multi-party computation - privacy va xavfsizlik muammolarining innovatsion yechimlari bo'lib, kelajakda keng qo‘llanishi kutilmoqda.

Xulosa

Face ID tizimlarida biometrik ma’lumotlarni shifrlash va saqlash zamonaviy kiberxavfsizlikning eng muhim yo‘nalishlaridan biri hisoblanadi. Tadqiqot natijalari shuni ko‘rsatadiki, biometrik ma’lumotlarning noyob xususiyatlari ularni himoya qilish uchun maxsus kriptografik yondashuvlarni talab qiladi.

Face ID texnologiyasida biometrik ma’lumotlar xavfsizligi - bu faqat texnik masala emas, balki foydalanuvchilar ishonchi, business reputation va regulatory compliance masalasidir. Muvaffaqiyatli implementatsiya uchun technical expertise, adequate investment va long-term security strategy talab etiladi.

Zamonaviy Face ID tizimlari bir necha qatlamli himoya tizimini qo‘llaydi: hardware darajasida Secure Enclave yoki TEE muhitlari, dasturiy ta’minot darajasida AES shifrlash va ECC algoritmlari, shuningdek, template darajasida irreversible transformatsiya usullari. Bu yondashuvlar biometrik ma’lumotlarning maxfiyligini va yaxlitligini yuqori darajada ta’minlaydi.

Biroq, texnologiyaning rivojlanishi bilan birga yangi tahdidlar ham paydo bo‘lmoqda. Shuning uchun biometrik himoya texnologiyalari doimiy takomillashtirishni talab qiladi. Kelajakda quantum kriptografiya, homomorph shifrlash va AI asosidagi himoya tizimlari yanada keng qo‘llanilishi kerak.

Biometrik autentifikatsiya tizimlarining xavfsizligini ta‘minlash uchun texnik choralarga qo‘shimcha ravishda qonunchilik va etik normalarni ham hisobga olish zarur. Foydalanuvchilarning biometrik ma’lumotlari ustidan nazoratini kuchaytirish va shaffoflikni oshirish muhim vazifalar hisoblanadi.

Kelajakda biometrik autentifikatsiya yanada keng tarqalishi bilan, ushbu sohadagi xavfsizlik standartlari va best practicelar barcha stakeholderlar uchun kritik ahamiyat kasb etadi. Faqat comprehensive va forward-looking approach orqaligina biometrik texnologiyalarning barcha afzalliklaridan xavfsiz foydalanish mumkin bo‘ladi.

Face ID tizimlarida biometrik ma’lumotlarning xavfsizligini ta’minlash zamonaviy kiberxavfsizlikning eng muhim masalalaridan biridir.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Prezidenti. (2024-yil 24-may). “Ma’muriy islohotlar doirasida adliya organlari va muassasalarining mas’uliyatini yanada oshirish hamda ixcham boshqaruv tizimini shakllantirish to‘g‘risida”gi farmoni. – Toshkent.
2. Qodirov, F. (2022). Kiberxavfsizlik va kompyuter tizimlarini himoya qilish. – Toshkent: “Fan va texnologiya” nashriyoti.
3. Shodmonov, Sh. (2021). Axborot texnologiyalari va axborot xavfsizligi asoslari. – Toshkent: “Iqtisodiyot” nashriyoti.

4. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2023). Raqamli xavfsizlik strategiyasi 2023–2030. – Toshkent.

5. Karimov, A. (2020). Axborot xavfsizligi va kriptografiya asoslari. – Toshkent: O‘zbekiston Milliy universiteti nashriyoti.

6. Raxmonqulov, I. (2019). Biometrik texnologiyalar va ularning qo‘llanilishi. – Toshkent: “Innovatsiya” nashriyoti.

7. O‘zbekiston Respublikasi Vazirlar Mahkamasi. (2023). “Raqamli O‘zbekiston – 2030” strategiyasini amalga oshirish chora-tadbirlari to‘g‘risida qaror. – Toshkent.

8. Vahobov, A.V., Malikov, T.S. (2012). Moliya. – Toshkent: Iqtisod-moliya nashriyoti. (Axborot xavfsizligiga oid moliyaviy jihatlar tahlili uchun).

9. Usmonov, N. (2021). Kriptografik algoritmlar va ularning amaliy qo‘llanilishi. – Toshkent: TATU nashriyoti.

10. O‘zbekiston Respublikasi Adliya vazirligi. (2024). Davlat xizmatlarini ko‘rsatishda biometrik autentifikatsiya tizimlarini joriy etish bo‘yicha uslubiy qo‘llanma. – Toshkent.