BIOMETRIK BARMOQ IZI ORQALI AXBOROTLAR XAVFSIZLIGI

Ro‘zaliyev Abdumalikjon Vahobjon o‘g‘li
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali magistranti

R.Adaxanov
"O‘zbektelekom" AK Farg‘ona filiali

Umarov Abdumuxtor Maxammad o‘g‘li
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali magistranti

ANNOTATSIYA

Bugungi tahlikali axborot asri davridagi muammolar juda ko‘payib kelmoqda. Ushbu maqolada axborot timizlari foydalanuvchilarining xavfsizligi ta’minlashdan iboratdir. Axborot tizimlari foydalanuvchilarining shu kungacha parol orqali tizimga kirish ommalashgan. Buning o‘rninga foydalanuvchilarning biometrik autentifikatsiyasi orqali tizim foydalanuvchilarining xavfsizligi darjasi yuqori ko‘rsatkichga ega. Biz bu tizimni ishga tushurish orqali foydalanuvchilar xavfsizligi ta’minlangan bo‘ladi.

Kalit so‘zlar: biometrik, biometrik autentifikatsiya, axborot tizimlari, barmoq izi, axborot tizimlari foydalanuvchilari.

Asosiy qism

Hozirgi tahlikali davrdagi ma’lumotlarga bo‘lgan xavfsizlikga talab yuqori bo‘lmoqda. Shaxsni tasdiqlovchi ungan tegishli boshqa ma’lumotlarni saqlashning barmoq izi orqali saqlashni ushbu maqolada tanlab oldim. Xususan har bir insonning yuz tuzulishi, ko‘z qorachig‘i va boqmoq izi o‘zgarmas hisoblanadi. Bular orqali axborot tizmlariga kirishdagi bosqichlar bularni kiritishni talab qilib qo‘yadigan bo‘lsak bu ko‘rinib turibdiki ma’lumotlarni xavsizligi ta’minlagan bo‘lamiz. Bu

jarayonlarni amalga Shirish uchun bizdan mablag‘ talab qilishi turgan gap bularga barmoq izini skayner(o‘qib oladigan) qurilma va yuz shaklini aniqlash uchun yuqori sifatli video kamera talab etiladi.

Biometrik - bu o‘zgarmas o‘ziga xos tug‘ma biologik belgilar bo‘yicha shaxsni aniqlash. Bu texnologiyalarga asoslangan kirish va axborotni himoya qilish tizimlari nafaqat eng ishonchli, balki bugungi kunda foydalanuvchilar uchun eng qulay. Eng muhimi shundaki siz murakkab parollarni yodlashingiz shart emas, doimiy ravishda siz bilan apparat kalitlari yoki aqlli karta(elektron raqamli imzo, feshka yozilgan kuluch)larni olib yurishingiz kerak. Barmog‘ingizni skanerlash orqali axborot tizimlariga kirish yetarli bo‘ladi, bunda boshqa bir shaxsni kirishini oldi olingan bo‘ladi.

Barcha biometrik tizimlar bir diagrammada ishlaydi. Dastlab yozish jarayoni natijasida tizim biometrik xususiyatlarni eslaydi. Ba'zi biometrik tizimlar biometrik xususiyatlarning yanada batafsil ishlab chiqilishi uchun bir nechta namunalarni yaratadi. Olingan ma'lumotlar qayta ishlanadi va matematik kodga aylantiriladi. Biometrik axborot xavfsizligi tizimlari biometrik identifikatsiya usullaridan va foydalanuvchi autentifikatsiyasidan foydalanadi. Biometrik tizimni aniqlash to‘rt bosqichda amalga oshiriladi:

- Identifikatorni ro‘yxatdan o‘tkazish - fiziologik yoki xulq-atvor xususiyatlarini kamaytirish kompyuter texnologiyalari uchun mavjud bo‘lgan shaklga aylantirilib, biometrik tizimga keltiriladi;
- Tanlov - yangi taqdim etilgan identifikatordan tizim tomonidan tahlil qilingan noyob xususiyatlar ajratiladi;
- Taqqoslash - yangi taqdim etilgan va ilgari ro‘yxatdan o‘tgan identifikator to‘g‘risidagi ma'lumotlar taqqoslanadi;
- Echim - yangi taqdim etilgan identifikator tasodif yoki to‘g‘ri kelmaydimi yoki yo‘qmi degan xulosa qilinadi.

Biometrik texnologiyalar asosida axborotni himoya qilish tizimlarining muhim xususiyatlaridan biri bu yuqori ishonchlilik, ya'ni tizimning turli odamlarga tegishli

biometrik xususiyatlarini ishonchli tarzda ajratish va tasodiflarni ishonchli deb bilish qobiliyati. Biometrikalarda ushbu parametrlar birinchi turdagi xato (noto‘g‘ri rad etish darajasi, FRR) va ikkinchi turdagi xato (yolg‘on qabul qilish darajasi, uzoq). Birinchi raqam odamga kirish huquqiga ega bo‘lish ehtimolini tavsiflaydi, ikkinchisi ikki kishining biometrik xususiyatlarining yolg‘on tasodifining ehtimolligi ehtimolidir. Soxta odam papillilar naqsh yoki kamalak ko‘z qobig‘i juda qiyin. Shunday qilib, "ikkinchi turdagi xatolar" ning paydo bo‘lishi (ya'ni bunga huquqi bo‘lmagan shaxsga kirish) deyarli chiqarib tashlanadi. Biroq, ba'zi omillarning ta'siri ostida, identifikatsiyani aniqlashning biologik xususiyatlari farq qilishi mumkin. Masalan, odam sovuqni ushlashi mumkin, natijada uning ovozi tan olinishdan tashqari o‘zgaradi. Shuning uchun biometrik tizimlarda "birinchi turdagi" xatolar paydo bo‘lishining chastotasi (unga tegishli shaxsga kirishdan bosh tortish) katta. Tizim bir xil qiymatlar bilan FRR qiymatidan yaxshiroqdir. Qiyosiy xususiyatlar Ilon (teng xato darajasi), bu FRR va ancha grafik kesishish nuqtasini belgilaydi. Ammo bu har doim vakillikdan uzoqdir. Biometrik tizimlardan foydalanganda, hatto to‘g‘ri biometrik xususiyatlar har doim joriy qilinmasa ham, autentifikatsiya qarori to‘g‘ri. Bu bir qator xususiyatlar va birinchi navbatda, biometrik xususiyatlar farq qilishi mumkinligi bilan bog‘liq. Ma'lum bir darajadagi tizim xatolari mavjud. Bundan tashqari, turli xil texnologiyalardan foydalanganda xatolar sezilarli darajada farq qilishi mumkin. Kirish boshqaruv tizimlari uchun biometrik texnologiyalardan foydalanganda, "musofir" ni o‘tkazib yubormaslik yoki "ularni" o‘tkazib yuborish uchun nima muhimligini aniqlash kerak.

Barmoq izlarini autentifikatsiya qilish. Barmoq izlarini aniqlash eng keng tarqalgan, ishonchli va samarali biometrik texnologiya hisoblanadi. Ushbu texnologiyaning ko‘p qirraliligi tufayli uni deyarli har qanday sohada qo‘llanilishi va ishonchli foydalanuvchi identifikatsiyasi zarur bo‘lgan har qanday vazifani hal qilish mumkin. Usul barmoqlardagi kapillyar naqshlar naqshining o‘ziga xosligiga asoslanadi. Maxsus skaner, sensor yoki sensor bilan olingan chop etish raqamli kodga aylantiriladi va ilgari kiritilgan ma'lumotnoma bilan taqqoslanadi.

Har bir insonning barcha barmoqlarining bosmalari papiller chiziqlar chizishida noyobdir va hatto egizaklarda ham farq qiladi. Barmoq izlari kattalar hayoti davomida o‘zgarmaydi, ular osonlikcha va identifikatsiyalanishda shunchaki taqdim etiladi.

Agar barmoqlardan biri shikastlangan bo‘lsa, siz "Zavod" bosmalarini aniqlash uchun foydalanishingiz mumkin, ularning tafsilotlari, shuningdek, biometrik tizimda foydalanuvchilarni ro‘yxatga olish bilan ham kiradi.

Barmoq izlari barmoq izlarini olish uchun ixtisoslashtirilgan skanerlar qo‘llaniladi. Barmoq izlarini skanerlashning uchta asosiy turi mavjud: Kuctivititiv, aylanadigan optik.

Barmoq izlari uchun eng zamonaviy identifikatsiya texnologiyasi optik skanerlar tomonidan amalga oshiriladi.

Afzallik va kamchiliklar. Biometrik axborotni himoya qilish tizimlarining eng katta kambamasi narxi. Va bu so‘nggi ikki yil ichida turli xil skanerlar narxi sezilarli darajada pasayganiga qaramay. To‘g‘ri, biometrik qurilmalar bozori bo‘yicha tanlov kurashi tobora qiyin shakllarga aylanmoqda. Va shuning uchun narxni qisqartirish kutilmoqda. Biometrikaning boshqa etishmasligi ba'zi skanerlarning juda katta hajmidir. Tabiiyki, bu barmoq izi va boshqa parametrlardagi shaxsni aniqlashga taalluqli emas. Bundan tashqari, ba'zi hollarda umuman maxsus qurilmalar mavjud emas. Kompyuterni mikrofon yoki veb-kamk bilan jihozlash kifoya.

Xulosa. Bugungi tahlikali axborot asri davridagi muammolar juda ko‘payib kelmoqda. Ushbu maqolada axborot timizlari foydalanuvchilarining xavfsizligi ta’minlashdan iboratdir. Axborot tizimlari foydalanuvchilarining shu kungacha parol orqali tizimga kirish ommalashgan. Buning o‘rninga foydalanuvchilarning biometrik autentifikatsiyasi orqali tizim foydalanuvchilarining xavfsizligi taminlash yuqori hisoblanadi. Boshqichma bosqich biz shu jarayonlarni tadbiq etadigan bo‘lsak buzib kiruvchilarni ishini to‘xtatgan bo‘lamiz yani ma’lumotimiz xavfsiz saqlanadi. Bunga talab bugungi kuda juda yuqori. Axborot xavfsizligi sohasida barmoq izi orqali ma’lumotlarni saqlash eng yuqori sanaladi.

FOYDALANILGAN ADABIYOTLAR: (REFERENCES)

1. Axborot xavfsizligi(kitob) Muallif M.M Karimov, K.A.Tashev, S.K.Ganiyev Toshkent 2017

2. Kiberxavfsizlik asoslari(o‘quv qo‘llanma). S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov Toshkent 2020

3. Методы повышения эффективности систем биометрической аутентификации пользователей информационных систем по изображению лица. кандидат наук: Волкова Светлана Сергеевна

4. Диссертация Разработка и исследование биометрических методов и средств защиты информации: БАЙРБЕКОВА ҒАЗИЗА СЕРІККЫЗЫ. Алматы, 2017

5. **Biometric authentication: assuring access to information** Harris, A.J. and Yen, D.C.

6. Secure Biometric Authentication with Improved Accuracy Manuel Barbosa, Thierry Brouard

7. http://tizim.nammqi.uz/elektron-kutubxona/fayl//AXBOROTXAVFSIZLIGIPDF.pdf

8. https://whatsappss.ru/uz/utilities/biometricheskie-sistemy-zashchity-informacii-vidy-biometricheskie-sistemy-zashchity.html

9. https://newtravelers.ru/uz/asus/klassifikaciya-biometricheskih-sistem-zashchity-informacii-osnovy.html