AXBOROT TIZIMLARIDAN FOYDALANISHNING BIOMETRIK NAZORATLASH ALGORITMLARI VA VOSITALARINI ISHLAB CHIQISH MEXANIZMLARI

G’ofurova Madina Ikromjon qizi
Toshkent amaliy fanlar universiteti
1-bosqich talabasi
gafurova0504.@gmail.com

Annotatsiya: Ushbu maqola axborot tizimlaridan foydalanishning biometrik nazoratlash algoritmlari va vositalarini ishlab chiqish masalalariga bag‘ishlangan. Maqolada biometrik nazorat tushunchasi, uning axborot xavfsizligidagi roli, turli biometrik identifikatsiya usullari (barmoq izi, yuzni tanish, iris skanerlash, ovoz orqali identifikatsiya va h.k.) haqida umumiy ma’lumotlar berilgan. Shuningdek, maqolada biometrik nazoratlash algoritmlarining asosiy prinsiplari, ishlash mexanizmlari, afzalliklari va kamchiliklari tahlil qilinadi. Maqolada biometrik vositalarni axborot tizimlariga integratsiya qilish jarayoni va ularning samaradorligini oshirishga qaratilgan algoritmik yondashuvlar ham ko‘rib chiqilgan. Mazkur tadqiqot natijalari axborot tizimlarida xavfsizlikni kuchaytirish va foydalanuvchi autentifikatsiyasini optimallashtirish bo‘yicha amaliy tavsiyalar beradi.

Kalit so‘zlar: Biometrik nazorat, axborot tizimi, autentifikatsiya, identifikatsiya algoritmlari, foydalanuvchi tekshiruvi, xavfsizlik, barmoq izi skaneri, yuzni tanish tizimi, iris skanerlash, ovoz orqali identifikatsiya, biometrik ma’lumotlar, tizim integratsiyasi, ma’lumotlar himoyasi.

Kirish. Zamonaviy axborot texnologiyalari hayotimizning barcha sohalariga kirib kelgan davrda axborot tizimlarida ma’lumotlarni himoya qilish va tizimlardan foydalanishni nazorat qilish masalasi dolzarb ahamiyat kasb etadi. Axborot tizimlariga ruxsatsiz kirish, foydalanuvchi ma’lumotlarining o‘g‘irlanishi yoki buzilishi xavfi kundan-kunga oshib bormoqda. Shu sababli, tizimlarning xavfsizligini ta’minlash va

foydalanuvchi autentifikatsiyasini samarali tashkil etish eng muhim vazifalardan biri hisoblanadi. Biometrik nazoratlash – foydalanuvchining shaxsiy biologik yoki xulq-atvor xususiyatlariga asoslangan identifikatsiya va autentifikatsiya jarayoni bo‘lib, u axborot tizimlarida foydalanuvchining shaxsini aniqlash va tizimga kirishni nazorat qilish imkonini beradi. Ushbu yondashuv odatiy parollar yoki tokenlardan farqli o‘laroq, foydalanuvchining noyob biologik xususiyatlariga asoslanadi, shuning uchun xavfsizlik darajasi yuqori bo‘ladi. Biometrik nazoratlashning asosiy usullari qatoriga barmoq izi skanerlash, yuzni tanish tizimi, iris skanerlash va ovoz orqali identifikatsiya kiradi. Har bir usul foydalanuvchining biometrik ma’lumotlarini yig‘ish, saqlash, solishtirish va tizimga kirishini avtomatlashtirishga yordam beradi. Shu bilan birga, biometrik algoritmlar axborot tizimlarining xavfsizligini oshirish, ruxsatsiz kirishni oldini olish va foydalanuvchi qulayligini ta’minlash imkonini beradi.[1] Biometrik nazorat – bu foydalanuvchining biologik yoki xulq-atvor belgilariga asoslangan autentifikatsiya jarayoni bo‘lib, u axborot tizimlarida foydalanuvchining shaxsini aniqlash va tizimga kirishni nazorat qilish imkonini beradi.

Axborot tizimlarida biometrik nazoratning eng asosiy vazifalaridan biri foydalanuvchining shaxsini aniqlashdir. Bu jarayon tizimga kirayotgan shaxs haqiqatan ro‘yxatga olingan foydalanuvchi ekanligini tasdiqlashga xizmat qiladi.[2] An’anaviy autentifikatsiya usullari, masalan, parol yoki token, ma’lumotlarni himoya qilishda yetarli darajada ishonchli bo‘lmasligi mumkin, chunki parolni buzish yoki tokendan foydalanishni taqlid qilish mumkin. Shu sababli biometrik usullar foydalanuvchining noyob biologik yoki xulq-atvor xususiyatlariga, masalan, barmoq izi, yuz shakli, iris naqshi yoki ovoziga asoslanadi. Bu usullar yuqori aniqlik darajasiga ega bo‘lib, foydalanuvchini tizimga kirishda aniqlash jarayonini samarali qiladi. Shu bilan birga, foydalanuvchi shaxsini aniqlash tizim xavfsizligini ta’minlashning birinchi va eng muhim bosqichi hisoblanadi. Biometrik nazoratning ikkinchi muhim vazifasi tizimga ruxsatsiz kirishni oldini olishdir.

[1] Foydalanilgan adabiyot nomini yozish kerak

[2] Foydalanilgan adabiyot nomini yozish kerak

Oddiy parol yoki tokenlar foydalanuvchi shaxsini tekshirishda yetarli darajada xavfsizlikni ta’minlay olmasligi mumkin. Biometrik ma’lumotlardan, masalan, barmoq izi, yuz shakli yoki iris naqshidan foydalanish orqali, tizimga kirish jarayoni yanada ishonchli bo‘ladi. Bu yondashuv ruxsatsiz kirishni sezilarli darajada kamaytiradi, chunki biometrik xususiyatlarni soxta nusxa orqali taqlid qilish juda qiyin. Shu tariqa, biometrik nazorat axborot tizimining xavfsizlik darajasini oshiradi va ma’lumotlarning noqonuniy o‘qilishi yoki o‘g‘irlanishining oldini oladi.[3] Biometrik nazorat tizimlari foydalanuvchi harakatlarini monitoring qilish imkoniyatini ham ta’minlaydi. Bu vazifa tizimda kim qaysi ma’lumotga kirganini aniqlash va xavfsizlik protokollarini kuzatishga xizmat qiladi. Masalan, foydalanuvchi tizimga kirganda uning biometrik ma’lumotlari orqali shaxs aniqlanadi va tizimda qilgan harakatlari qayd qilinadi. Bu audit jarayonini soddalashtiradi, ruxsatsiz harakatlarni tez aniqlashga yordam beradi va tizimdagi xavfsizlik holatini real vaqt rejimida nazorat qilish imkonini beradi. Shu bilan birga, foydalanuvchi monitoringi yordamida tizim samaradorligi va ishlash jarayoni yaxshilanadi. Biometrik nazoratning yana bir muhim vazifasi foydalanuvchining ma’lumotlarini himoya qilishdir. Biometrik ma’lumotlar foydalanuvchining shaxsiy identifikatsiyasini ta’minlaydi va tizimdagi ma’lumotlarga kirishni nazorat qiladi. Shu orqali shaxsiy ma’lumotlar xavfsiz saqlanadi, ruxsatsiz foydalanishning oldi olinadi va ma’lumotlarni himoya qilish darajasi oshadi. Biometrik ma’lumotlar shifrlangan holda saqlanadi, bu esa ularni o‘g‘irlanish yoki noto‘g‘ri foydalanish xavfidan himoya qiladi. Shu tariqa, biometrik nazorat axborot tizimlarida ma’lumotlarni xavfsiz saqlash va tizim ishonchliligini ta’minlashning samarali vositasi sifatida xizmat qiladi.

Biometrik nazoratning eng muhim afzalliklaridan biri – foydalanuvchini aniqlashdagi yuqori aniqlik va ishonchliligi hisoblanadi. Har bir insonning biometrik xususiyatlari, masalan, barmoq izi, iris naqshi yoki yuz tuzilishi, noyob bo‘lib, ularni soxta nusxa orqali taqlid qilish deyarli imkonsizdir. Shu sababli, biometrik tizimlar foydalanuvchini noto‘g‘ri tanib olish xavfini sezilarli darajada kamaytiradi va tizimning

[3] Foydalanilgan adabiyot nomini yozish kerak

xavfsizlik darajasini oshiradi.[4] Biometrik nazorat foydalanuvchi uchun juda qulay hisoblanadi. Parol yoki tokenlarni yodlash, ularni doimiy yangilab borish kabi murakkab jarayonlar bilan solishtirganda, foydalanuvchi biometrik ma’lumotlarini oddiy usulda taqdim etadi. Masalan, tizimga kirish uchun faqat barmoq izini skanerlash yoki yuzni tanitish kifoya qiladi. Bu foydalanuvchi tajribasini yaxshilaydi va tizimdan foydalanishni osonlashtiradi.

Barmoq izi skanerlash biometrik identifikatsiya usullari orasida eng keng qo‘llaniladigan va eng ishonchli texnologiyalardan biridir. Har bir insonning barmoq izlari noyob bo‘lib, hayot davomida o‘zgarmaydi. Axborot tizimlarida barmoq izi skanerlash foydalanuvchining barmog‘ini skaner qurilmasiga qo‘yish orqali amalga oshiriladi.[5] Skaner barmoqdagi xatoliklar, bo‘g‘imlar va naqshlarni aniqlab, saqlangan ma’lumotlar bilan solishtiradi. Biometrik algoritmlar ushbu naqshlarni raqamli shablonlarga aylantirib, ma’lumotlar bazasidagi moslikni tekshiradi. Agar barmoq izi mos kelsa, foydalanuvchiga tizimga kirish huquqi beriladi. Ushbu usulning afzalligi – yuqori aniqlik va ruxsatsiz kirishni sezilarli darajada kamaytirishdir. Yuzni tanish tizimi kameralar va maxsus dasturiy ta’minot orqali foydalanuvchining yuzini aniqlashga asoslanadi. Tizim foydalanuvchining yuz konturini, ko‘zlar, burun, lablar va yuzning boshqa geometrik xususiyatlarini tahlil qiladi. Algoritmlar bu xususiyatlar orasidagi masofalarni va shakllarni raqamli shablon sifatida saqlaydi. Tizimga kirishda foydalanuvchi yuzini kamera orqali skaner qilganda, dastur ushbu shablonlarni ma’lumotlar bazasidagi shablonlar bilan solishtiradi.[6] Agar moslik aniqlansa, foydalanuvchi tizimga kiradi. Yuzni tanish tizimi foydalanuvchiga qulaylik yaratadi, parol yoki token talab qilmaydi va tezkor autentifikatsiya imkonini beradi. Shu bilan birga, tizim yorug‘lik, yuz ifodalari va kamera sifatiga bog‘liq holda aniqlik darajasi o‘zgarishi mumkin. Iris skanerlash ko‘zning iris qismidagi noyob naqshlarni aniqlashga asoslangan. Iris naqshlari har bir inson uchun individual bo‘lib,

[4] Foydalanilgan adabiyot nomini yozish kerak

[5] Foydalanilgan adabiyot nomini yozish kerak

[6] Foydalanilgan adabiyot nomini yozish kerak

hayot davomida deyarli o‘zgarmaydi.[7] Axborot tizimlarida iris skanerlash qurilmasi foydalanuvchining ko‘zini skanerlaydi va irisdagi naqshlarni raqamli formatga aylantiradi. Algoritmlar ushbu naqshlarni ma’lumotlar bazasidagi shablonlar bilan solishtiradi va autentifikatsiya jarayonini amalga oshiradi. Iris skanerlash yuqori xavfsizlik va aniqlik darajasi bilan ajralib turadi, shuning uchun maxsus xavfsizlik talab qilinadigan tizimlarda keng qo‘llaniladi. Shu bilan birga, bu usul foydalanuvchining qulayligi jihatdan biroz cheklangan, chunki skanerga ko‘zni aniq joylashtirish talab etiladi. Ovoz orqali identifikatsiya foydalanuvchining ovoz xususiyatlariga asoslangan biometrik usuldir. Algoritmlar foydalanuvchining ovoz ohangi, ritmi, talaffuzi va boshqa fonetik xususiyatlarini tahlil qiladi. Tizim foydalanuvchi ovozini ma’lumotlar bazasida saqlangan ovoz namunasi bilan solishtiradi. Agar ovoz mos kelsa, tizim foydalanuvchiga kirish huquqini beradi.[8] Ushbu usul masofadan autentifikatsiya qilish imkonini beradi va qulay interfeys bilan foydalanuvchi tajribasini oshiradi. Shu bilan birga, ovoz orqali identifikatsiya atrof-muhit shovqini, kasallik yoki tovush o‘zgarishlariga bog‘liq holda aniqlik darajasi pastlash xavfini tug‘diradi.

Tahlil. Biometrik nazoratlash vositalarini axborot tizimlariga muvaffaqiyatli integratsiya qilish bir necha bosqichdan iborat bo‘lib, har bir bosqich tizimning xavfsizligi va foydalanuvchi autentifikatsiyasining samaradorligini ta’minlashga xizmat qiladi.

Biometrik vositalarni integratsiya qilish jarayoni tizim xavfsizlik talablarini aniqlashdan boshlanadi. Bu bosqichda tizimga kirish darajasi, foydalanuvchi autentifikatsiyasi va monitoringning qanchalik qat’iy bo‘lishi belgilanishi kerak. Masalan, bank tizimlari yoki davlat muhim ma’lumotlar bazalari uchun autentifikatsiya yuqori darajada qat’iy bo‘lishi zarur bo‘lsa, oddiy korporativ tizimlarda xavfsizlik talablarining o‘rtacha darajasi yetarli bo‘lishi mumkin. Shu bilan birga, xavfsizlik darajasi

[7] Foydalanilgan adabiyot nomini yozish kerak

[8] Foydalanilgan adabiyot nomini yozish kerak

foydalanuvchi qulayligi bilan uyg‘unlashishi ham muhimdir, chunki ortiqcha murakkab autentifikatsiya jarayoni foydalanuvchi tajribasini pasaytiradi.

Keyingi bosqichda foydalanuvchilarning biometrik ma’lumotlari yig‘iladi va maxfiylikni ta’minlash sharti bilan saqlanadi. Bu ma’lumotlar barmoq izi, yuz, iris yoki ovoz kabi biometrik xususiyatlarni o‘z ichiga oladi. Ma’lumotlar shifrlangan formatda saqlanishi kerak, bu ularning ruxsatsiz foydalanish yoki o‘g‘irlanish xavfini sezilarli darajada kamaytiradi. Shu bilan birga, saqlash tizimi foydalanuvchi identifikatsiyasini tezkor va aniq amalga oshirish imkonini beradigan tarzda optimallashtiriladi.

Biometrik ma’lumotlar yig‘ilgandan so‘ng, har bir biometrik vosita va identifikatsiya algoritmi tizim bilan moslashtiriladi. Bu jarayon algoritmlarning tizimning mavjud dasturiy va apparat infratuzilmasi bilan muvofiqligini ta’minlaydi. Misol uchun, barmoq izi skaneri, yuzni tanish tizimi yoki iris skanerlash algoritmlari axborot tizimining autentifikatsiya moduli bilan uzviy ishlashi kerak. Algoritmlarning tizim bilan to‘liq uyg‘unlashuvi foydalanuvchining biometrik ma’lumotlari real vaqt rejimida tez va aniq tekshirilishini kafolatlaydi.[9]

Oxirgi bosqich foydalanuvchi tizimga kirganda biometrik ma’lumotlarni real vaqt rejimida tekshirishni o‘z ichiga oladi. Bu jarayonda foydalanuvchi biometrik ma’lumotini taqdim qiladi, tizim esa oldindan saqlangan shablonlar bilan solishtirib, autentifikatsiyani amalga oshiradi. Agar moslik aniqlansa, foydalanuvchiga tizimga kirish huquqi beriladi. Shu bilan birga, tizim har qanday shubhali kirish urinishini qayd qiladi va xavfsizlik protokollarini ishga tushiradi.

Biometrik nazoratlash axborot tizimlarida foydalanuvchi autentifikatsiyasini samarali tashkil etish va tizim xavfsizligini oshirishda muhim vosita hisoblanadi. Ushbu texnologiyaning bir qancha **afzalliklari** mavjud bo‘lib, ular tizimni foydalanuvchi uchun qulay va ishonchli qiladi. Birinchidan, biometrik nazoratlashning asosiy afzalligi — yuqori aniqlik va ishonchlilikdir. Biometrik xususiyatlar, masalan, barmoq izi, iris naqshi yoki yuz tuzilishi har bir inson uchun noyob bo‘lib, ularni soxta nusxa orqali taqlid qilish deyarli

[9] Foydalanilgan adabiyot nomini yozish kerak

imkonsizdir. Shu sababli, biometrik tizimlar foydalanuvchini aniqlashda xato qilish ehtimolini sezilarli darajada kamaytiradi va tizim xavfsizligini oshiradi. Ikkinchidan, biometrik nazoratlash tizimga kirish jarayonini tezlashtiradi. An'anaviy parol yoki tokenlardan farqli ravishda foydalanuvchi tizimga kirish uchun faqat o'zining barmoq izi, yuzini tanitish yoki ovozini taqdim etadi. Bu jarayon tez va intuitiv bo'lib, foydalanuvchi tajribasini sezilarli darajada yaxshilaydi. Uchinchidan, biometrik tizimlar ruxsatsiz kirish xavfini kamaytiradi. Biometrik ma'lumotlar noyobligi tufayli tizimga ruxsatsiz kirish, firibgarlik yoki ma'lumotlarni o'g'irlash ehtimoli sezilarli darajada pasayadi. Shu tariqa, axborot tizimlarining xavfsizligi mustahkamlanadi. To'rtinchidan, biometrik nazoratlash foydalanuvchi uchun qulay va intuitiv tizim yaratadi. Parolni eslab qolish yoki tokenlardan foydalanish shart emas; foydalanuvchi tabiiy xususiyatlari orqali tizimga kiradi. Bu esa foydalanuvchi tajribasini oshiradi va tizimdan foydalanishni soddalashtiradi.[10]

Shuningdek, biometrik nazoratlashning ba'zi **kamchiliklari** ham mavjud. Birinchidan, biometrik ma'lumotlar o'g'irlanishi xavfi saqlanadi. Agar ma'lumotlar yetarli darajada himoyalanmasa, ruxsatsiz shaxslar ushbu ma'lumotlardan foydalanishi mumkin. Shu sababli, biometrik ma'lumotlarni shifrlash va xavfsiz saqlash alohida e'tibor talab qiladi. Ikkinchidan, texnik jihatdan nosozliklar va noto'g'ri aniqlash holatlari yuz berishi mumkin. Masalan, barmoq izi skaneri ifloslangan bo'lsa, yuzni tanish tizimi yomon yorug'lik sharoitida ishlasa yoki foydalanuvchi ovozi o'zgarsa, autentifikatsiya jarayoni muvaffaqiyatsiz bo'lishi mumkin. Uchinchidan, biometrik ma'lumotlarni saqlash va himoya qilish uchun qo'shimcha resurslar talab qilinadi. Shifrlash, xavfsiz saqlash va tizim monitoringi uchun apparat va dasturiy ta'minot resurslari qo'shimcha xarajatlarni keltirib chiqaradi.[11] Shu bilan birga, biometrik nazoratlashning afzalliklari kamchiliklarga qaraganda ko'proq bo'lib, zamonaviy axborot tizimlarida foydalanuvchi autentifikatsiyasi va ma'lumotlar xavfsizligini ta'minlashda muhim vosita hisoblanadi.

[10] Foydalanilgan adabiyot nomini yozish kerak

[11] Foydalanilgan adabiyot nomini yozish kerak

Tahlil va natijalar. Zamonaviy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash va foydalanuvchi autentifikatsiyasini samarali tashkil etish dolzarb masala hisoblanadi. Ushbu maqolada biometrik nazoratlash algoritmlari va vositalari tahlil qilindi hamda ularning axborot tizimlariga integratsiya qilish jarayoni, afzalliklari va kamchiliklari batafsil ko‘rib chiqildi.

Biometrik nazoratlash foydalanuvchining biologik yoki xulq-atvor xususiyatlariga asoslangan identifikatsiya va autentifikatsiya jarayonini o‘z ichiga oladi. Asosiy usullar – barmoq izi skanerlash, yuzni tanish tizimi, iris skanerlash va ovoz orqali identifikatsiya – yuqori aniqlik, tezkorlik va foydalanuvchi qulayligini ta’minlaydi. Shu bilan birga, biometrik algoritmlar foydalanuvchi ma’lumotlarini saqlash, shifrlash va tizimga kirishni avtomatlashtirishga xizmat qiladi. Biometrik vositalarni axborot tizimlariga integratsiya qilish jarayoni bir nechta bosqichlardan iborat: tizim xavfsizlik talablarini aniqlash, biometrik ma’lumotlarni yig‘ish va shifrlash, algoritmlarni tizim bilan moslashtirish va real vaqt rejimida autentifikatsiya jarayonini amalga oshirish. Ushbu bosqichlarning har biri tizim xavfsizligi va foydalanuvchi autentifikatsiyasini samarali ta’minlash uchun muhimdir. Biometrik nazoratlashning afzalliklari aniq: yuqori aniqlik va ishonchlilik, tizimga kirish jarayonini tezlashtirish, ruxsatsiz kirish xavfini kamaytirish va foydalanuvchi uchun qulay tizim yaratish. Shu bilan birga, biometrik ma’lumotlarning o‘g‘irlanishi xavfi, texnik nosozliklar va qo‘shimcha resurs talab qilinishi kabi kamchiliklari ham mavjud. Biroq, samarali xavfsizlik protokollari va ma’lumotlarni himoya qilish mexanizmlari orqali ushbu kamchiliklar sezilarli darajada kamaytirilishi mumkin.[12]

Umuman olganda, biometrik nazoratlash axborot tizimlarida foydalanuvchi autentifikatsiyasi va ma’lumotlar xavfsizligini ta’minlashning samarali va ishonchli vositasi sifatida ajralib turadi. Biometrik texnologiyalarni to‘g‘ri tanlash, algoritmlarni optimallashtirish va tizimlarga integratsiya qilish orqali axborot tizimlarining ishonchliligi va xavfsizligini sezilarli darajada oshirish mumkin.

12

Foydalanilgan adabiyotlar

1. Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer.

2. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Springer.

3. Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). *Biometric Identification*. IEEE Computer Society.

4. Kumar, A., & Zhang, D. (2005). *Personal Recognition Using Multiple Biometric Traits*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(3), 450–455.

5. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). *Enhancing Security and Privacy in Biometrics-Based Authentication Systems*. IBM Systems Journal, 40(3), 614–634.

6. Fierrez, J., Ortega-Garcia, J., & Gonzalez-Rodriguez, J. (2007). *Biometric Systems: Technology, Design and Performance Evaluation*. Springer.

7. Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). *Biometric Systems: Technology, Design and Performance Evaluation*. Springer.

8. Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). *Biometric Cryptosystems: Issues and Challenges*. Proceedings of the IEEE, 92(6), 948–960.

9. ISO/IEC 19794-2:2005. *Information technology – Biometric data interchange formats – Part 2: Finger minutiae data*. International Organization for Standardization.