FOYDALANUVCHILARNI BIOMETRIK IDENTIFIKATSIYALASH VA AUTENTIFIKATSIYALASH

Po’latov Doston Normurod o’g’li
Yoqubova Madinabonu Abdushukur qizi
Torebaeva Naziyra
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Biometrik identifikatsiya va autentifikatsiya, foydalanuvchilarni boshqa ma'lumotlardan farq qiladigan va ularga yuqori darajada xavfsizlik ta'minlayan bir usuldur. Ushbu usul, foydalanuvchining biometrik xususiyatlarini (masalan, qo'llarini, yuzini, qo'llab-quvvatlangan imzolarini yoki retinalarini) ishlatib, ularning identifikatsiyasini va autentifikatsiyasini amalga oshiradi.*

Kalit so’zlar:*Biometrik identifikatsiya, autentifikatsiya, xavfsizlik, qulaylik, intuitivlik, avtomatlashtirish, biometrik xususiyatlar, yuqori daraja, falsifikatsiya, parol, kod, identifikatsiya, autentifikatsiya, xatolik darajasi.*

Abstract: *Biometric identification and authentication is a method that differentiates users from other data and provides them with a high level of security. This method uses biometric features of the user (such as hands, face, supported signature or retina) to identify and authenticate them.*

Keywords: *Biometric identification, authentication, security, convenience, intuitiveness, automation, biometric features, high level, falsification, password, code, identification, authentication, error rate.*

Biometrik identifikatsiya va autentifikatsiyalashning afzalliklari va kamchiliklari quyidagicha bo'lishi mumkin:

KIRISH

Foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash, kriptografiya sohasidagi innovatsion tamoyillardan biridir. Bu usul, insonning biometrik ma'lumotlarini (masalan, uning ot, qo'l, yuz yoki qo'lparmak izi) foydalanib identifikatsiya va autentifikatsiyani amalga oshirishni ta'minlaydi.

Biometrik identifikatsiya, foydalanuvchining shaxsiy biometrik ma'lumotlarini tarqatish yordamida uning to'g'ri shaxsni aniqlashga imkon beradi. Bu ma'lumotlar, foydalanuvchining biometrik xususiyatlarini ifodalaydi va uning shaxsiy identifikatsiyasini ta'minlaydi. Misol uchun, bir telefonni ochishda qo'l izidan foydalanish bilan telefon foydalanuvchisini biometrik ravishda tanishib olish mumkin.

Biometrik autentifikatsiya esa foydalanuvchining shaxsiy biometrik ma'lumotlarini foydalanib, uning to'g'ri shaxsni tasdiqlashga imkon beradi. Bu usul, parol yoki kalit so'z kabi traditsionallik qo'llashga alternativa bo'lib foydalanuvchini xavfsizlik va ishonchni

oshiradi. Misol uchun, bankomatga kirishda yuz tanishish tizimi yordamida foydalanuvchi o'zini tasdiqlaydi.

Biometrik identifikatsiya va autentifikatsiyalashning afzalliklari va kamchiliklari bilan birga, ularning bir nechta muhim masalalari ham mavjud. Ularning davomida quyidagilar o'zgartirilishi mumkin:

1. Xavfsizlikning o'rnatilishi: Biometrik identifikatsiya va autentifikatsiya tizimlari foydalanuvchining jismoniy xususiyatlari bilan ishlaydi va bu xususiyatlar unikallashtirilgan ma'lumotlarga aylanadi. Bu narsalar tizimga xakerlarni nishonlaydi va foydalanuvchining maxfiylikini ta'minlaydi.

2. Isrofni kamaytirish: Biometrik identifikatsiya va autentifikatsiya tizimlari foydalanuvchilar uchun oson va tezkor bo'lishini ta'minlaydi. Ular uchun parol yoki kalit so'z yodlashga va uning tiklanishini kuzatishga kerak emas.

3. Ishonchli foydalanish: Biometrik xususiyatlar foydalanuvchining unikalligini ifodalaydi va uni takrorlash qiyin. Bu tizimlarni ishonchli foydalanishga imkon beradi, chunki foydalanuvchi jismoniy xususiyatlarini kuzatib borayotgan tizimning o'ziga ishonadi.

4. Soddalik va qulaylik: Biometrik identifikatsiya va autentifikatsiya tizimlari foydalanuvchilar uchun oson va qulay bo'lishini ta'minlaydi. Ularning ishlash jarayonlari oson va avtomatik tarzda amalga oshiriladi, shuningdek foydalanuvchilar uchun qulay va oson bo'lgan foydalanish tajribasi yaratadi.

5. Xususiy sohalarda qo'llanish: Biometrik identifikatsiya va autentifikatsiya tizimlari mahsulotlarini bir qancha sohalarda qo'llash mumkin. Masalan, telefonlar, bankomatlar, kompyuterlar, sayohat va imkoniyatlar tizimlari kabi muhitlarda foydalanish imkoniyatini beradi.

Shundan tashqari, biometrik identifikatsiya va autentifikatsiya tizimlari ham yuqori narxga ega bo'lishi, har qanday tekshiruv va ta'minot jarayonlari talab qilishi va har qanday texnik muammo va nusxalanuvchilik muammo bilan bog'liq kamchiliklarga ega bo'lishi mumkin.

AFZALLIKLAR:

1. Yuqori darajada xavfsizlik: Biometrik xususiyatlar shaxsiy va unikal xususiyatlardan tashkil topadi, shuning uchun falsifikatsiya va o'zgartirishlarga qarshi yuqori darajada himoya qilinadi.

2. Qulay va intuitiv: Foydalanuvchilar uchun biometrik identifikatsiya va autentifikatsiya oson va qulaydir, ular uchun parollar yodlashga va xotiradan foydalanishga zarur emas.

3. Avtomatik ish: Biometrik tizimlar foydalanuvchilar uchun avtomatik ishlaydi, ularga boshqa xususiyatlarga qaraganda tezroq va ishonchli tizimga kirish imkonini beradi.

KAMCHILIKLAR:

1. Maxfiylik muammolari: Biometrik ma'lumotlar himoyalangan o'zgarishmaydigan xususiyatlardan tashkil topadi, shuning uchun ularni himoya qilish uchun yaxshi amaliyotlar va maxfiylik standartlarini ta'minlash zarur.

2. Xatoliklar: Biometrik identifikatsiya va autentifikatsiya tizimlari, biometrik xususiyatlarni to'g'ri o'qib olmay olish, ko'payib ketish yoki noto'g'ri tan olish kabi xatoliklarga yo'l qo'yishi mumkin.

3. Istisno holatlarda ishlash kamchiligi: Biometrik tizimlar, biometrik xususiyatlarni to'g'ri bilan olishni talab qiladi. Ba'zida, biometrik xususiyatlar yetarli ravishda o'qilmay, masalan, katta qasosiylik, yuzni qismen yopish, yoki yoqolish kabi holatlarda tizimlar to'g'ri ishlamay oladi.

Bu afzalliklar va kamchiliklar, biometrik identifikatsiya va autentifikatsiyalashning muhim muammo va asosiy masalalari bo'lib, ularni qo'llashda va amalga oshirishda ehtiyotkorlik va diqqat bilan amal qilish kerak.

Biometrik identifikatsiya va autentifikatsiyalash misollaridan ba'zi quyidagilardir:

1. Parmaq izi skaneri: Foydalanuvchining parmaq izi bilan identifikatsiya va autentifikatsiya qilinishi mumkin. Parmaq izi skaneri, parmaq izini o'qib oladi va uni ma'lumotlar bazasidagi parmaq izlari bilan taqqoslaydi.

2. Yuz tan olish: Yuz tan olish tizimi, foydalanuvchining yuzidagi xususiyatlarni tan olish va uning identifikatsiya va autentifikatsiyasini ta'minlash uchun ishlatiladi. Tizim, yuzni skaner orqali o'qib oladi va uning unikal xususiyatlari bilan taqqoslaydi.

3. Retina skaneri: Retina skaneri, foydalanuvchining retina qopqog'ida o'qib olgan xususiyatlarni identifikatsiya va autentifikatsiyaga asoslash uchun ishlatiladi. Skaner, retina tomonidan yaratilgan unikal qopqog'ini skanlaydi va uning ma'lumotlar bazasidagi ma'lumotlar bilan taqqoslaydi.

4. Quloq izi skaneri: Quloq izi skaneri, foydalanuvchining quloq izidagi xususiyatlarni identifikatsiya va autentifikatsiyaga asoslash uchun ishlatiladi. Skaner, quloq izini o'qib oladi va uning ma'lumotlar bazasidagi ma'lumotlar bilan taqqoslaydi.

5. Iris skaneri: Iris skaneri, foydalanuvchining irisida yaratilgan unikal xususiyatlarni o'qib oladi va ularni identifikatsiya va autentifikatsiyaga asoslaydi. Skaner, irisning unikal xususiyatlarini skanlaydi va ma'lumotlar bazasidagi ma'lumotlar bilan taqqoslaydi.

Bu misollar, biometrik identifikatsiya va autentifikatsiyalashning bir necha turdagi tizimlardan faqat bir qismidir. Boshqa turdagi biometrik tizimlar ham mavjud bo'lib, har biri o'zining afzalliklari va kamchiliklari bilan ajralib turadi.

Biometrik identifikatsiya va autentifikatsiyalash tizimlari bilan bog'liq ba'zi muammo va masalalar mavjud:

1. Faraziylik: Biometrik identifikatsiya va autentifikatsiyalash tizimlari, biometrik ma'lumotlarni asoslash uchun foydalanuvchining iste'mol etishiga bog'liq. Bunda, foydalanuvchi biometrik ma'lumotlarni boshqa tizimlarga ko'chirish, soxta to'lov va hakam etishlardan himoya qilinishi zarur.

2. Xavfsizlik va farovonlik: Biometrik ma'lumotlar himoyalangan bo'lsa ham, ularga hujum qilish mumkin. Misol uchun, parmaq izi skanerlari, qulaylik uchun ishlatilayotgan tarzda soxta parmaq izlarining qabul qilinishi mumkin.

3. Faraziylik: Biometrik ma'lumotlar shaxsiy xususiyatlarga asoslanganligi uchun, foydalanuvchilarning ma'lumotlarini faraziylik bilan saqlash va uni noto'g'ri ishlatish imkoniyati mavjud. Bu, ma'lumotlar himoyalashning katta muammo bo'lib, qat'iyan yechilishi kerak.

4. Ma'lumotlar bazasi xavfsizligi: Biometrik identifikatsiya va autentifikatsiyalash ma'lumotlar bazalari yaratilishi va saqlanishi bilan bog'liq xavfsizlik muammolarini o'z ichiga oladi. Bu ma'lumotlar bazalari yorqin himoya qilinishi, sirli kalit so'zlar bilan muxofaza qilinishi va hujum va soxta to'lovlar bilan muhofaza qilinishi kerak.

5. Faraziylikni uchun kichik sondirish: Biometrik identifikatsiya va autentifikatsiyalash tizimlarining faraziylik darajasini oshirish uchun, ikkita faraziy ma'lumotni bir vaqtda o'zgartirish talab qilinadi. Bu ma'lumotlar o'zgarishi uchun ma'lumotlar bazasiga qat'iy himoya talab qilinadi.

Biometrik identifikatsiya va autentifikatsiyalashning muammolariga yechim topish uchun texnologik rivojlanish, xavfsizlik protokollari va foydalanuvchilar bilan ta'lim muhimdir. Muammolar ustida yaxshi tahlil va loyihalar ishlab chiqilishi kerak, shuningdek, faraziylik, ma'lumotlar bazasi xavfsizligi va farovonlikning muhofazasi uchun yaxshi amaliyotlarni amalga oshirish kerak.

Xulosa:Biometrik identifikatsiya va autentifikatsiya, foydalanuvchilarni identifikatsiya qilish va autentifikatsiya qilishning yuqori darajada xavfsiz va qulay usullaridan biridir. Ushbu usul, foydalanuvchining biometrik xususiyatlarini ishlatib, ularning shaxsiy identifikatsiyasini va autentifikatsiyasini amalga oshiradi. Biometrik xususiyatlar, shaxslar tomonidan qullanishga mo'ljallangan qo'llanma, yuz, retina, qo'llab-quvvatlangan imza kabi shaxsiy ma'lumotlardan tashkil topadi.

FOYDALANILAGAN ADABIYOTLAR:

1. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

2.«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

3. «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

4. С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

5.S.S.Qosimov. Axborot texnologiyalari. 0‘quv qoMlanma. - T.: «Aloqachi», 2006.

6.S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.