AXBOROT TIZIMLARIDA PAROLSIZ AUTENTIFIKATSIYA: YUZNI TANISH VA BIOMETRIK KIBERXAVFSIZLIK METODLARI

Mirzo Ulug’bek nomidagi

O’zbekiston Milliy universiteti Jizzax filiali

Xudoyqulova Fotima

Guruh:263-24

Axborot tizimlari va texnologiyalari yo’nalishi

Annotatsiya. Mazkur ishda axborot tizimlarida parolsiz autentifikatsiya texnologiyalari, ayniqsa yuzni tanish asosidagi biometrik identifikatsiya usullari va ularning kiberxavfsizlikdagi ahamiyati tahlil qilinadi. Biometrik autentifikatsiya foydalanuvchini identifikatsiyalashning eng qulay va xavfsiz usullaridan biri bo‘lib, phishing va parol o‘g‘irlanishi kabi hujumlarni kamaytiradi. Shu bilan birga, biometrik ma’lumotlarni himoyalash, *spoofing* hujumlarini aniqlash va *liveness detection* algoritmlarini qo‘llash zarurati ko‘rib chiqiladi.

Kalit so‘zlar: parolsiz autentifikatsiya, biometrika, yuzni tanish, liveness detection, spoofing, kiberxavfsizlik, identifikatsiya.

Аннотация. В данной статье анализируются технологии беспарольной аутентификации в информационных системах, в частности методы биометрической идентификации на основе распознавания лиц, и их значение в кибербезопасности. Биометрическая аутентификация является одним из наиболее удобных и безопасных методов идентификации пользователя, снижающим риск таких атак, как фишинг и кража паролей. Одновременно рассматривается необходимость защиты биометрических данных, обнаружения атак с подделкой и применения алгоритмов проверки подлинности.

Ключевые слова: беспарольная аутентификация, биометрия, распознавание лиц, проверка подлинности, подмена данных, кибербезопасность, идентификация.

Raqamli xizmatlarning kengayishi bilan foydalanuvchi autentifikatsiyasi axborot tizimlarining eng muhim xavfsizlik komponentiga aylandi. An’anaviy autentifikatsiya usuli — login va parol — inson omiliga bog‘liq bo‘lgani sababli zaif hisoblanadi. Parollarni eslab qolish qiyinligi, qayta ishlatilishi va fishing hujumlari tufayli hisoblar buzilishi keng tarqalgan.

Shu sababli zamonaviy axborot tizimlarida passwordless authentication — parolsiz autentifikatsiya konsepsiyasi joriy etilmoqda. Bu usul foydalanuvchini biometrik belgilar orqali aniqlaydi va inson xatosiga bog‘liqlikni kamaytiradi.

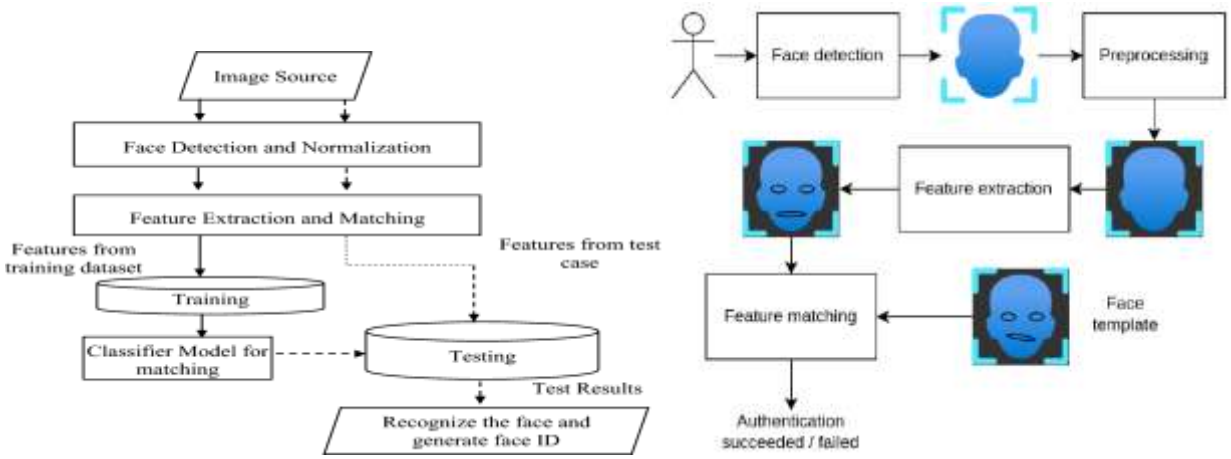
Parolsiz autentifikatsiya tushunchasi

Autentifikatsiya — tizim foydalanuvchining haqiqiyligini tekshirish jarayonidir. Zamonaviy xavfsizlik modelida autentifikatsiya uch omilga asoslanadi:

1. Bilimga asoslangan (parol, PIN)
2. Egalikka asoslangan (token, smart-karta)
3. Biometrik asoslangan (yuz, barmoq izi, iris)

Parolsiz autentifikatsiya uchinchi omilga asoslanib, foydalanuvchi shaxsiy biologik xususiyatlarini tekshiradi.

Yuzni tanish texnologiyasining ishlash prinsipi



Yuzni tanish tizimi kompyuter ko‘rish va sun’iy intellekt algoritmlariga asoslanadi. Jarayon quyidagi bosqichlardan iborat:

1. Face detection – tasvirdan yuzni aniqlash
2. Feature extraction – yuzning geometrik parametrlarini ajratish
3. Template creation – matematik model yaratish
4. Matching – ma’lumotlar bazasi bilan taqqoslash

Ushbu jarayonlar natijasida tizim foydalanuvchi shaxsini tasdiqlaydi yoki kirishni rad etadi.

Biometrik autentifikatsiya xavflari va kiberxavfsizlik metodlari

Biometrik tizimlar yuqori xavfsizlik darajasini ta'minlasa-da, ularga xos bo‘lgan ma'lum xavflar mavjud:

Spoofing va Deepfake: Foto, video replay, 3D maskalar yoki sun’iy intellekt yordamida yaratilgan soxta tasvirlar orqali tizimni aldashga urinishlar.

Ma’lumot sizishi: Biometrik ma’lumot o‘g‘irlangan taqdirda, paroldan farqli o‘laroq, uni almashtirib bo‘lmaydi.

Texnik xatoliklar: Noto‘g‘ri ruxsat berish (FAR) va noto‘g‘ri rad etish (FRR) ko‘rsatkichlari bilan bog‘liq muammolar.

Ushbu xavflarni bartaraf etish uchun quyidagi himoya metodlari qo‘llaniladi:

Liveness detection: Foydalanuvchining "tirikligini" aniqlash uchun ko‘z qimirlatish, bosh harakati, infraqizil kameralar va chuqurlik sensorlaridan foydalaniladi.

Shifrlangan shablonlar: Serverda foydalanuvchining haqiqiy yuz tasviri emas, balki uning shifrlangan matematik modeli yoki hash-qiymati saqlanadi.

Ko‘p omilli autentifikatsiya: Biometrika qo‘shimcha ravishda qurilma yoki kriptografik kalit bilan mustahkamlanadi.

Biometrik identifikator Tekshiruv texnologiyalari bugungi kunda xavfsizlik va sog'liqni saqlashdan tortib moliya va ta'limgacha bo'lgan ko'plab sohalarda keng qo'llaniladi. Ushbu texnologiyalar jismoniy yoki xulq-atvor xususiyatlaridan foydalangan holda shaxslarni aniqlash va tekshirish jarayonini avtomatlashtiradi. Biometrik tizimlar an'anaviy usullarga nisbatan xavfsizroq va amaliy muqobil taklif qiladi, bu esa foydalanuvchilar hayotini osonlashtiradi, shu bilan birga firibgarlik va shaxsiy ma'lumotlarni o'g'irlash kabi xavflarni kamaytirishga yordam beradi.

Biometrik tizimlar tomonidan taqdim etilgan aniqlik va xavfsizlik afzalliklari ularni ayniqsa, nozik ma'lumotlarni himoya qilishni talab qiladigan sohalarda afzal ko'rdi. Masalan, bank operatsiyalarida barmoq izlari yoki yuzni tanishdan foydalangan holda autentifikatsiya qilish ruxsatsiz kirishning oldini olish orqali mijozlar xavfsizligini oshiradi. Xuddi shunday, aeroportlarda ishlatiladigan ìrísí tanib olish tizimlari xavfsizlik zaifliklarini minimallashtirish bilan birga pasport nazorati jarayonlarini tezlashtiradi.

Parolsiz autentifikatsiya zamonaviy axborot tizimlarida eng istiqbolli himoya mexanizmlaridan biri hisoblanadi. Yuzni tanish texnologiyasi qulaylik va xavfsizlikni birlashtiradi, biroq uni qo‘llashda liveness detection, shifrlash va ko‘p omilli autentifikatsiya kabi qo‘shimcha himoya choralarini qo‘llash zarur. Kompleks yondashuvgina biometrik autentifikatsiyaning ishonchliligini ta’minlaydi.

С расширением цифровых услуг аутентификация пользователей стала важнейшим компонентом безопасности информационных систем. Традиционный метод аутентификации — логин и пароль — считается слабым, поскольку зависит от человеческого фактора. Взлом учетных записей широко распространен из-за сложности запоминания паролей, их повторного использования и фишинговых атак.

Поэтому в современных информационных системах внедряется концепция аутентификации без пароля. Этот метод идентифицирует пользователя по биометрическим характеристикам и снижает зависимость от человеческой ошибки.

Концепция аутентификации без пароля

Аутентификация — это процесс проверки подлинности пользователя системой. В современной модели безопасности аутентификация основана на трех факторах:

1. На основе знаний (пароль, PIN-код)

2. На основе владения (токен, смарт-карта)

3. На основе биометрии (лицо, отпечаток пальца, радужная оболочка глаза)

Аутентификация без пароля основана на третьем факторе — проверке личных биологических характеристик пользователя.

Принцип работы технологии распознавания лиц

Системы распознавания лиц основаны на алгоритмах компьютерного зрения и искусственного интеллекта. Процесс состоит из следующих этапов:

1. Обнаружение лица – идентификация лица по изображению

2. Извлечение признаков – извлечение геометрических параметров лица

3. Создание шаблона – создание математической модели

4. Сопоставление – сравнение с базой данных

В результате этих процессов система подтверждает личность пользователя или отказывает в доступе.

Риски биометрической аутентификации и методы кибербезопасности

Хотя биометрические системы обеспечивают высокий уровень безопасности, с ними связаны определенные риски:

Подмена данных и дипфейки: попытки обмануть систему с помощью фотографий, видеозаписей, 3D-масок или искусственно сгенерированных поддельных изображений.

Утечка данных: в отличие от паролей, биометрические данные не могут быть восстановлены в случае кражи.

Технические ошибки: проблемы с ложными авторизациями (FAR) и ложными отклонениями (FRR).

Для устранения этих рисков используются следующие методы защиты:

Определение живости: движения глаз, движения головы, инфракрасные камеры и датчики глубины используются для определения того, «жив» ли пользователь.

Зашифрованные шаблоны: на сервере хранится зашифрованная математическая модель или хеш лица пользователя, а не фактическое изображение лица пользователя.

Многофакторная аутентификация: биометрические данные дополнительно усиливаются устройством или криптографическим ключом.

Технологии биометрической идентификации и верификации сегодня широко используются во многих отраслях, от безопасности и здравоохранения до финансов и образования. Эти технологии автоматизируют процесс идентификации и проверки личности на основе физических или поведенческих характеристик. Биометрические системы предлагают более безопасную и практичную альтернативу традиционным

методам, упрощая жизнь пользователям и помогая снизить такие риски, как мошенничество и кража личных данных. Точность и безопасность биометрических систем сделали их особенно популярными в отраслях, требующих защиты конфиденциальных данных. Например, аутентификация с использованием отпечатков пальцев или распознавания лиц в банковских операциях повышает безопасность клиентов, предотвращая несанкционированный доступ. Аналогично, системы распознавания радужной оболочки глаза, используемые в аэропортах, ускоряют процессы паспортного контроля, минимизируя при этом уязвимости в системе безопасности.

Беспарольная аутентификация — один из наиболее перспективных механизмов защиты в современных информационных системах. Технология распознавания лиц сочетает в себе удобство и безопасность, но её использование требует дополнительных мер защиты, таких как проверка подлинности, шифрование и многофакторная аутентификация. Только комплексный подход обеспечивает надежность биометрической аутентификации.

Foydalanilgan adabiyotlar

1. NIST Digital Identity Guidelines (SP 800-63B)

2. ISO/IEC 30107-3 Biometric Presentation Attack Detection

3. OWASP Authentication Cheat Sheet

4. Jain, Ross, Prabhakar — Introduction to Biometrics

5. Ratha et al. — Enhancing security and privacy in biometrics