



ÓBUDAI EGYETEM

**Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet**

SZAKDOLGOZAT

**ÓE-KGK
2023**

Hallgató neve:
Hallgató törzskönyvi száma:

**Ullmann Gábor József
T007199/FI12904/G**



SZAKDOLGOZAT FELADATLAP¹

Hallgató neve: Ullmann Gábor József

Törzskönyvi száma: T007199/FI12904/G

Neptun kódja: [REDACTED]

Tagozat: Nappali

Szak: Gazdaságinformatikus

Specializáció: Vállalatinformatikai

A dolgozat címe: A bankkártyával történő fizetés biometrikus kiváltásának vizsgálata

A dolgozat címe angolul: Investigation of the replacement of the credit cards by biometric identification

Feladat:

1. Végezzen elméleti kutatást a biometrikus azonosítás megoldásairól, és azok bankkártyával történő fizetést kiváltó lehetőségeiről
2. Végezzen primer kutatást a bankkártyás fizetés biometrikus kiváltásának lehetőségéről
3. Tegyen javaslatot, mely azonosítást és hogyan lehetne alkalmazni bankkártyás fizetés helyettesítésére.
4. Összegezze a kapott kutatási eredményeket, vonjon le következtetéseket, valamint fogalmazzon meg további kutatási lehetőségeket!

Intézményi konzulens neve: Bálint Krisztián

A kiadott téma elévülési határideje: 1 év

Beadási határidő: 2023. 12. 15.

A záróvizsga tárgyai: Gazdaságinformatika, Vállalatinformatikai

A szakdolgozat titkos / nem titkos

Kiadva: Budapest, 2023. 10. 09.

P. H.

.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találok:

.....
Intézményi konzulens

¹ A végleges **Szakdolgozat feladatlapot** a szakirányának megfelelő intézet állítja ki. Ezt a végleges **Szakdolgozat feladatlapot** kell beköttetnie!



HALLGATÓI NYILATKOZAT

Alulírott Ullmann Gábor József (Neptunkód: ████████) hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2023. 12. 15.

hallgató aláírása

Tartalomjegyzék

1.	BEVEZETÉS	7
1.1.	Témaválasztás indoklása	8
1.2.	Téma relevanciája	8
1.3.	Tanulmány célja	8
1.4.	Hipotézisek.....	9
1.5.	Kutatási módszertan.....	9
2.	BIOMETRIKUS AZONOSÍTÁSI LEHETŐSÉGEK	10
2.1.	Arcfelismerés	12
2.2.	Ujjlenyomat.....	14
2.3.	Írisz azonosítás	17
2.4.	Retina azonosítás.....	19
3.	EMPIRIKUS KUTATÁS	20
4.	HIPOTÉZISEK IGAZOLSÁSA, ELVETÉSE.....	31
5.	BANKKÁRTYÁK KIVÁLTÁSA BIOMETRIKUS AZONOSÍTÁSSAL A GYAKORLATBAN	33
5.1.	Hol használható fel a kutatás eredménye	33
5.2.	Javaslatok	34
5.3.	További kutatási lehetőség.....	44
6.	ÖSSZEFOGLALÁS	46
	IRODALOMJEGYZÉK	48

TARTALMI KIVONAT.....	I
-----------------------	---

SUMMARY.....	I
--------------	---

ÁBRAJEGYZÉK

1. ábra: Az arc jellemzőinek felmérése	13
2. ábra: Az ujjlenyomatok globális és lokális jellemzői	16
3. ábra: A már valahol biometrikus azonosítást használók aránya	22
4. ábra: Z generáció biometrikus azonosításra váltásra való hajlandósága.....	23
5. ábra: A megkérdezettek tranzakció idejüknek hossza	25
6. ábra: A készpénz és a bankkártya használatának eloszlása a kitöltők között	26
7. ábra: A biometrikus azonosítás kényelmessége a kitöltők szerint	27
8. ábra: Biometrikus azonosítási preferenciák.	29
9. ábra: Rendelkezik-e biometrikus azonosításra képes telefontal.....	30

TÁBLÁZATOK JEGYZÉKE

1. táblázat: Néhány biometrikus azonosítási módszer pontossága	11
2. táblázat: A kérdőív kitöltőinek generáció szerinti eloszlása	21
3. táblázat: Hipotézisek összesítése.	32

1. BEVEZETÉS

A pénzügyi szektorban napjainkban tapasztalható technológiai forradalom során egyre növekvő figyelmet kapnak az innovatív azonosítási megoldások, melyek célja a pénzügyi tranzakciók és fizetési rendszerek hatékonyságának és biztonságának fokozása. Ebben a kontextusban egy különleges terület került a figyelem középpontjába: a bankkártyák biometrikus azonosítással történő kiváltása.

Az előrehaladott biometrikus technológiák, mint például az ujjlenyomat- és arcfelismerés, nem csupán új dimenziókat nyitnak meg a pénzügyi tranzakciók biztonságában, hanem olyan felhasználói élményt is teremtenek, amely jelentősen eltér a hagyományos fizetési módszerektől. A biometrikus azonosítás térhódítása új paradigmát teremt a pénzügyi tranzakciókban, és ennek a középpontjában áll a bankkártyák biometrikus azonosítással történő kiváltása.

A következő fejezetekben részletes elemzést nyújtok a különböző biometrikus azonosítási módszerek működéséről és pontosságáról, miközben bemutatom, hol találkozhatunk ma is ezen technológiákkal a mindennapjaink alkalmával. Az áttekintést követően megvizsgálom ezeknek a rendszereknek a felhasználói elfogadottságát. Egy primer kutatás során a résztvevőkkel különböző biometrikus azonosítási módszereket értékelek, figyelembe véve többek között az elfogadottságot és kényelmet.

Az empirikus kutatás eredményei alapján kitérek arra, melyik biometrikus azonosítási módszer mutatkozik a leginkább elfogadottnak és alkalmazhatónak a mindennapi életünkben, különös tekintettel a bankkártyák kiváltására. A javaslat részében konkrét lépéseket ismertetek, amelyek szükségesek a kiválasztott biometrikus azonosítási módszer sikeres implementálásához.

Ezen átfogó megközelítés célja, hogy átfogó képet nyújtson a biometrikus azonosítások jelenlegi állapotáról, azok elfogadtságáról, és megadja az irányt a hatékony implementációhoz, különös tekintettel a pénzügyi tranzakciókban való alkalmazásra.

1.1. Témaválasztás indoklása

A kutatásom témájának a bankkártyával történő fizetés biometrikus kiváltásának vizsgálatát választottam, mert engem személy szerint mindig is foglalkoztattak a mindennapos életet egyszerűbbé tevő technikák, mint például, hogy hogyan és milyen eszközök segítségével lehetne kiváltani a mindennapos életben használt tárgyakat akár egy telefonos funkció kereti között is. Ennek segítségével szükségtelenné válik magunknál hordozni a bankkártyánkat, ugyanis amennyiben fizetni szeretnénk online vagy akár helyben, abban az esetben elegendő lenne valamely biometrikus azonosítási módszer valamelyikén keresztül igazolni magunkat. Ezek az eljárások egyedi fizikai jellemzők felhasználásával azonosítják az embereket, ilyen jellemzők lehetnek például ujjlenyomatok, arcfelismerés, hangfelismerés, tenyérvénák, írisz vagy akár a retina. A biometrikus azonosításnak számos releváns alkalmazása van a mai világban.

1.2. Téma relevanciája

Napjainkban ez egy elég releváns témának mondható, mivel a modern technológia egyik kiemelkedő területéről beszélünk, amely a mindennapi életünkben is egyre növekvő fontossággal bír. A biometrikus azonosításnak számos alkalmazása van már a mai világban. A bankok is egyre jobban igyekeznek felhasználni ezeket a lehetőségeket az ügyfelek személyi azonosságának igazolására, hogy növeljék a felhasználók felismerését, valamint csökkentsék az automatikus támadások és visszaélések sikerességét. A legtöbb telefon már rendelkezik erre alkalmas funkcióval, például beépített ujjlenyomat érzékelővel, vagy arc alapú azonosítással. Az eszközök adta lehetőséget a nagyobb bankok applikációi már ki is használják az ügyfelek biometrikus azonosítással történő beléptetéshez.

1.3. Tanulmány célja

Kutatási célom:

- Megvizsgálni, hogy mennyire elfogadott a felhasználók körében a biometrikus azonosítás alkalmazása a bankkártyák helyett.

- Elemezni, milyen mértékben növeli vagy csökkenti a biometrikus azonosítás a felhasználók elégedettségét és kényelmét a pénzügyi tranzakciók során.
- Azonosítani, milyen mértékben javítja a biometrikus azonosítás a tranzakciók sebességét és hatékonyságát a hagyományos bankkártyás fizetésekhez képest.

1.4. Hipotézisek

- I. Feltételezhetően a Z generáció többsége elfogadóbb lenne a biometrikus azonosítással történő fizetéssel.
- II. Feltételezhetően növelhető lenne a vásárlási élmény a biometrikus bankkártya rutinszerű alkalmazása által, mivel az kényelmesebb és hatékonyabb azonosítást tesz lehetővé.
- III. Feltételezhetően a biometrikus azonosítás gyorsabbá teheti a fizetési tranzakciókat, mivel nem szükséges hosszú PIN-kódot vagy jelszót beírni.
- IV. Feltételezhetően a biometrikus azonosítási lehetőségek közül az ujjlenyomat azonosítást választaná a legtöbb ember a bankkártya kiváltására.

1.5. Kutatási módszertan

Kutatásomban primer kutatást alkalmaztam egy kérdőív formájában, amely során saját adatokat gyűjtöttem a hipotéziseim vizsgálatának érdekében.

A primer kutatás friss és naprakész adatokat szolgáltat, mivel a kutatók közvetlenül gyűjtik őket a vizsgálat időpontjában. Ez lehetővé teszi, hogy az eredmények relevánsak és aktuálisak legyenek. Mindemellett specifikus kérdésekre koncentrálnak, és olyan adatokat gyűjtését segíti elő, amely kifejezetten a vizsgált problémára vonatkoznak.

A kérdőívben csak zárt kérdések szerepeltek, amiknek számos előnye van. A zárt kérdések eredményei könnyen átalakíthatók számszerű adatokká, amelyek statisztikai elemzésekhez használhatók. Zárt kérdések általában egyszerűbben analizálhatók, mivel a válaszok előre meghatározott kategóriákba sorolhatók. Mindezek mellett könnyebb kitöltést biztosít. A résztvevőknek könnyebb lehet kitölteni egy felmérést zárt kérdésekkel, mivel a válaszlehetőségek meghatározottak, így feltételezhetően több ember

2. BIOMETRIKUS AZONOSÍTÁSI LEHETŐSÉGEK

Az innovációk és a technológia gyors fejlődése nemcsak átalakítja, hanem forradalmasítja is a pénzügyi szektort és a fizetési módokat. Ezen átalakulások közül kiemelkedik a biometrikus azonosítás elterjedése, amely számos területen, köztük a bankkártyás tranzakciók igazolásához is, forradalmi változásokat hoz. A biometrikus azonosítás olyan innovatív módszer, amely az egyedi fizikai jellemzők, mint például ujjlenyomat, szem vagy hang, felhasználásával teszi lehetővé a fizetési ügyletek azonosítását és megerősítését. A rendszer a hagyományos PIN-kódok vagy aláírások helyett a személyes biometrikus jellemzőket alkalmazza, amelyek egyediak és nehezen másolhatók. Ennek köszönhetően a biometrikus azonosítás nemcsak hatékonyabb, de biztonságosabb is lehet, mivel egyedülálló jellegzetességek alapján azonosítja és hitelesíti a tranzakciókat. Ezen túlmenően, a felhasználók számára kényelmesebb megoldást nyújt, mivel nem igényel memorizálást vagy külön kódokat, csupán a saját biometrikus adatainkat.

A biometrikus azonosításnak számos előnye van a pénzügyi szektorban, ahol azon túl, hogy növeli a tranzakciók biztonságát, gyorsabbá és egyszerűbbé is teszi a fizetéseket. Az elterjedése a mindennapi életben és a kereskedelmi tevékenységekben is felvet új lehetőségeket, és megnyitja az utat egy olyan digitális pénzügyi ökoszisztéma felé, amely még inkább a felhasználók kényelmére és a tranzakciók hatékonyságára fókuszál.

A különböző módszerek egyik kulcsfontosságú tényezője a rendszerek megbízhatósága. Ennek összehasonlítására a FAR, FRR és EER mérőszámokat használják. Az FAR, azaz False Accept Rate megmutatja, hogy a rendszer milyen arányban ítél meg egy jogosulatlan felhasználót jogosultként. Az FRR, vagyis False Reject Rate, ennek az ellenkezője, tehát azt szemlélteti, hogy milyen megoszlásban utasít el egy jogosult felhasználót. Ennek a két értékgörbék metszéspontja pedig az EER, ami az Equal Error Rate rövidítése [3]. A rendszerek pontosságának értékelése kiemelkedő jelentőségű az informatikai és technológiai területeken, különösen olyan alkalmazásokban, ahol a pontos azonosítás elengedhetetlen. Az alábbi eső táblázat részletes betekintést nyújt a rendszerek pontosságára vonatkozó adatokról, amelyek alapján értékelhetjük és összehasonlíthatjuk az egyes rendszereket:

Hangazonosítás	1: 50
Ujjlenyomat azonosítás	1: 500
Írisz azonosítás	1: 131 000
Retinaazonosítás	1: 10 000 000+

1. táblázat: Néhány biometrikus azonosítási módszer pontossága

Forrás: A biometrikus ujjnyomat azonosítás alkalmazásának új lehetőségei. Hadmérnök, 8, 1.

A fenti táblázat segítségével betekintést nyerünk a különböző rendszerek pontosságába. Ahogy azt le is olvashatjuk a hangazonosítás elég pontatlan, mivel annak alkalmazása esetén 50 azonosításra jut egy téves ítélet, míg az ujjlenyomat esetén 500-ra. Az írisz már szignifikánsan pontosabb, mint az előző két módszer a 131 ezer mérés utáni egy hibával és végül a retina alapú azonosítás már annyira pontos, hogy több mint 10 millió mérés esetén futhatunk bele egy hibába.

Ezen eltérések megfelelő megértése és figyelembevétele kiemelkedő fontosságú annak érdekében, hogy a rendszert optimálisan alkalmazzuk. A pontosság tekintetében felmerül az a fontos szempont, hogy a kisebb létszámú, néhány száz embert azonosító rendszerek esetében a magas fokú pontosság nem mindig elengedhetetlen feltétel. Az ilyen kisebb létszámú alkalmazásokban a rendszer hatékonyan működhet, még akkor is, ha nem éri el a tökéletes pontosságot. Ugyanakkor, amikor a biometrikus azonosításnak nagyobb létszámú populációt kell lefednie, például több százezer ember esetében, a rendszernek magasabb pontosságra van szüksége ahhoz, hogy hatékonyan kezelje az azonosítási folyamatokat és minimalizálja az esetleges hibákat. Ezért a megfelelő biometrikus azonosító rendszer kiválasztásánál elengedhetetlen figyelembe venni a célpopuláció méretét és a rendszer általános alkalmazási környezetét.

Fontos megemlíteni mindezek mellett néhány kihívást és aggodalmat ezen azonosítások kapcsán. Az adatvédelem és az etikai kérdések kulcsfontosságúak, és gondoskodni kell arról, hogy az azonosításhoz használt adatok megfelelően védettek legyenek. Az

adatvédelmi és jogi keretek kialakítása elengedhetetlen a személyes adatok védelme érdekében.

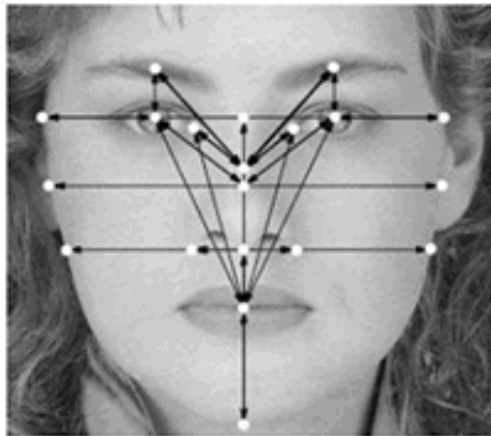
2.1. Arcfelismerés

Az arc alapú biometrikus azonosítás napjainkban egyre elterjedtebb és fontos technológiai fejlesztése, amely lehetővé teszi az egyedi azonosítást az emberi arc vonásainak és karakterisztikáinak felhasználásával. Ez a technológia a digitális világban és a fizikai biztonság területén is széles körben alkalmazható. Az ok nyilvánvaló, hiszen ez az úgynevezett passzív azonosítást lehetővé tevő eljárás a leginkább elfogadott biometrikus módszer, mert nem igényli a személy aktív közre működését, emellett gyors, és tömeg eseményeknél távoli azonosításra is alkalmazható [1]. A fenti tulajdonságok miatt könnyen elképzelhető, hogy a fokozott kényelem és felhasználói elfogadottság miatt az adott megoldás népszerűbb lehet más azonosítási módszerekkel szemben. Ugyanakkor fontos megjegyezni, hogy megbízhatóság szempontjából esetleg alulmarad más alternatívákhoz képest.

Ha az arc azonosítást összevetjük más biometrikus azonosítással, megállapítható, hogy az arc alapú azonosítás esetében a variabilitás, a pozíciók, a beállítások, a megvilágítás minősége, a gyűjtött, illetve a mintaképek felbontására, zajosságára való érzékenység nagy mértékben befolyásolja a rendszerek eredményességét [1]. Ez néhány esetben akár el is lehetetleníthetné a módszer alkalmazását, de már vannak megoldások, amelyek meg képesek birkózni az előbb említett akadályokkal. Telefonokban is megtalálhatóak ilyen megoldások, például a Face ID esetében. A folyamat során infravörös fényt bocsát ki, amelyet az emberi szem nem érzékel. Ez segít az arc kontúrjainak és jellemzőinek pontosabb megvilágításában, és lehetővé teszi a kamerának a háromdimenziós tér érzékelését.

Az arc azonosítás folyamata a következőképpen zajlik. Képfeldolgozás, képanalízis, amelynek első fontos lépése az arc felismerése a képen. Kamerák segítségével megtörténik a videó vagy az állóképek rögzítése, majd ezután különböző az arc azonosítást támogató speciális kép feldolgozási módszerekkel detektálja az azonosítandó ember arcát [1]. Ez a folyamat első kritikus lépése. Az arc felismerés folyamata komplex és magas technológiai színvonalat igényel, azonban az alkalmazott technológiai

megoldások folyamatos fejlődésben vannak, ezzel egyre hatékonyabb, pontosabb rendszerek alakulnak ki. Az arcnak a képen való megtalálása után, vagy akár avval párhuzamosan is, a rendszer soron következő feladata a képről származó biometrikus azonosításhoz szükséges mérendő és összehasonlítható tulajdonságok kivonása, összegyűjtése [1]. A kinyert sajátosságok olyan egyedi biometrikus jellemzőket alkotnak, melyek az arc különböző aspektusait ölelik fel. Ezek az egyediségek például az arc kontúryait, a szemöldökök elhelyezkedését, az orr és a száj vonalát foglalják magukba. Az ilyen biometrikus jellemzők azért rendkívül értékesek, mert egyedülállóak és különbözőek minden egyes egyénnél. Az alábbi első ábrán látható a vizsgálat során hogyan történik az arc ilyen jellemvonásainak feltérképezése:



1. ábra: Az arc jellemzőinek felmérése

Forrás: https://www.recoware.hu/biometria/biometria_i_azonositas/arc.html

Az ábra remekül szemlélteti, hogy az arc különböző jellemvonásait hogyan használja fel azonosításra. A távolságokat figyeli például a két orrcimpa között, a két szem közötti távolságot, a szem és a szemöldök távolságát és még sok egyéb ilyen vonást, ami alapján képes lesz döntést hozni.

Ebben a lépésben kiemelkedő kihívások közé tartozik az azonosítási hibák és a megtévesztés lehetősége. Például, olyan tényezők, mint a fényviszonyok változása, a viselt smink vagy az öregedés folyamata befolyásolhatja egy személy azonosítását, ami csökkentheti a pontosságát és megbízhatóságát. Az ilyen változók figyelembevétele és ezeknek a tényezőknek a korrigálása a biometrikus azonosítási rendszerek fejlesztésekor

kulcsfontosságú, hogy maximalizálni lehessen az azonosítás pontosságát és csökkenteni a hibalehetőségeket.

Az arc alapú biometrikus azonosítás széles körben használható, például a mobiltelefonokon, a laptopokon és az okostelefonokon történő feloldásnál, az épületek beléptetési rendszereiben, a banki tranzakcióknál és a repülőtereken a biztonsági ellenőrzéseknél. Ennek köszönhetően a mindennapi életünkben is egyre gyakrabban találkozhatunk ezzel a technológiával.

Léteznek kisebb, otthoni használatra tervezett rendszerek, amelyek kisebb, család méretű populációban képesek azonosításra. Ezen kívül vannak természetesen nagyobb populáción működő rendszerek is, (például kórházak betegfelvétele, számítástechnikai rendszerekhez történő beléptetés, bankok, kaszinók). A létező megoldások általában kis populációs rendszereknél, vagy más biometriai megoldásokkal ötvözve működnek sikeresen [2]. A különböző biometrikus azonosító rendszerek együttes használata miatt a tranzakciós folyamat időigényes lehet, ami érzékelhető különbséget eredményezhet az azonosítási sebesség és a hatékonyság tekintetében. Ez különösen fontos a pénzügyi tranzakciók terén, ahol a gyorsaság és az egyszerűség kiemelten fontosak az ügyfélélmény szempontjából. Az ügyfelek gyakran a gyorsaságot és a kényelmet értékelik a pénzügyi tranzakciók során, és ha a biometrikus azonosítás rendszerei összetettebbek vagy időigényesebbek, az visszatartó erő lehet azok elterjedésében.

2.2. Ujjlenyomat

Az ujjlenyomat azonosítás napjaink technológiai fejlődésének egyik csúcspontja, amely a személyazonosság megbízható és egyedi ellenőrzését teszi lehetővé. Az ujjlenyomatokat már évszázadok óta alkalmazzák a bűnüldözésben és az azonosításban, de a modern technológia lehetővé teszi számunkra, hogy digitálisan is használhassuk. Az okostelefonok és más eszközök ujjlenyomat-azonosítási funkciói például napjainkban széles körben elterjedtek, biztosítva az eszközök és az azokon tárolt személyes adatok védelmét. Rendkívül egyediek és személyre szabottak, hiszen minden egyes személy ujjlenyomata különbözik a többitől. Az ujjlenyomat azonosításnak számos előnye van a hagyományos azonosítási módszerekkel szemben. Könnyen rögzíthető, gyorsan

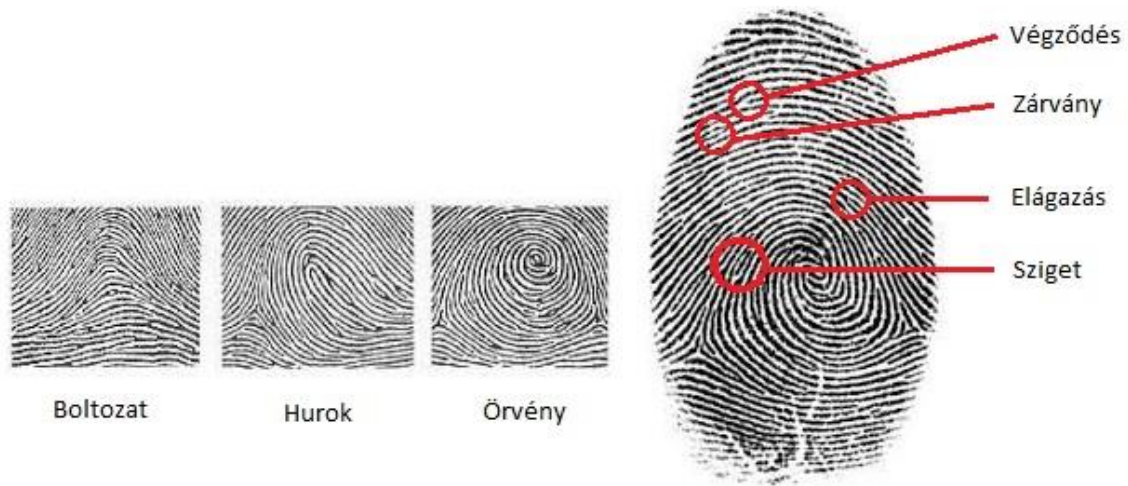
ellenőrizhető, és rendkívül nehéz másolni vagy hamisítani. Ezért a modern biztonsági rendszerek egyik sarkalatos elemévé vált az ujjlenyomat azonosítás.

A következőkben szeretnék tisztázni néhány fogalmat ezzel kapcsolatban. A daktiloszkópia három féle ujjról származó mintát különböztet meg: az ujjnyomot, az ujjlenyomatot és az ujjnyomatot. Az ujjnyom azokon a tárgyakon lelhető fel, amiket az ember megérint. Hiányosságuk miatt általában rossz minőségű képet adnak. Az ujjlenyomat az ujjról készült jó minőségű képek, amelyek az ujj utolsó ujjpercének teljes, körömtől-körömig tartó lenyomatát képezi. Ezt általában rendőrségi nyilvántartásokban használják. Végül az ujjnyomat a síkfelületre helyezett ujj ott maradó, kétdimenziós lenyomata. Ez többnyire jó minőségű, a személyazonosításban használatos [3]. Amikor tehát a mindennapokban használt ujjlenyomat azonosításról beszélünk, akkor valójában az ujjnyomatunkat vizsgálja a rendszer, és nem túl gyakran találkozunk ujjlenyomatokkal.

Ujjlenyomat alapján történő azonosítás esetében az ujjbegy mintázatát jegyzi fel, amely körülbelül 40–60 pontot jelent, de az érintett már mindössze 8–12 pont esetén is azonosítható, ugyanakkor a pontokból nem állítható helyre az eredeti ujjlenyomat, ezért a támogatói nem tartják ezt a módszert személyiségi jogokat sértőnek [4]. Az általunk vizsgált pontok számának növelése kulcsfontosságú tényező a korábban említett False Accept Rate (HAM - Helyes Elfogadás Aránya) és a False Reject Rate (HIR - Helytelen Elutasítás Aránya) görbéinek formálódásában. Ahogy a vizsgált pontok számát növeljük, észlelhető, hogy a False Accept Rate csökken, tehát a rendszer kevesebbszer fog helytelenül elfogadni egy azonosítási kísérletet. Azonban ezzel párhuzamosan a False Reject Rate is növekedni fog, ami azt jelenti, hogy több helyzetben következhet be helytelen elutasítás. A kiegyensúlyozás kialakítása rendkívül fontos, mivel a pontok számának optimalizálásának a célja a lehető legpontosabb azonosítás és az elfogadható hibaszint elérésének egyidejű biztosítása. A döntési küszöb beállítása és a rendszer finomhangolása során figyelembe kell venni ezeket az arányokat annak érdekében, hogy a biometrikus azonosítás hatékony és megbízható legyen a gyakorlati alkalmazások során.

Két fő biometriát alkalmaznak az azonosítás során: a minutiát és a mintázatot. Az előbb említett az ujjlenyomatok rajzolatában a különböző elágazásokat, rajzolat

megszakadásokat, hurkokat, kereszteződéseket és hidakat jelenti, az utóbbi pedig az ujjlenyomatok tipikus mintázatait [2]. Úgy is fogalmazhatnánk, hogy a minutia a lokális sajátosságai az ujjlenyomatoknak, a minta pedig a globális ismertetőjele. A kettő közötti különbséget a második ábra szemlélteti:



2. ábra: Az ujjlenyomatok globális és lokális jellemzői

Forrás: A biometrikus ujjnyomat azonosítás alkalmazásának új lehetőségei. Hadmérnök, 8, 1.

A globális jellemzők relatív gyakorisága eltérő, a boltozaté 3%, az örvényé 25%, a huroké pedig 72% [3]. Ez a százalékos megoszlás segít megérteni, hogy az egyes globális jellemzők milyen gyakran fordulnak elő az átlagos populációban. Az eltérő gyakoriságok alapján az ujjlenyomat-azonosítási rendszerek finomhangolhatók és optimalizálhatók, hogy még hatékonyabbak és megbízhatóbbak legyenek az egyedi azonosítás terén.

Egyre inkább teret hódít a mindennapos életben. Az épületek beléptető rendszerei is gyakran használnak ujjlenyomat-azonosítást, amely megkönnyíti a biztonságos belépést és a területek korlátozott hozzáférését. Ezenkívül az ujjlenyomatok szerepet játszanak a jogi és kormányzati területeken is, ahol rendőrségi nyilvántartásokban rögzítik őket a bűnügyi nyomozások és azonosítások céljából. Nem meglepő, hogy a számítógépes munkahelyek hozzáférését, csaknem kizárólag ujjlenyomat-azonosítókkal védik, a viszonylag alacsony költségek, kis méret és könnyű integrálhatóság miatt [2]. Magyarországon lehetőségünk van hozzárendelni személyi igazolványunkhoz az ujjlenyomatunkat. Ezt egyelőre leginkább repülőtereken használják. Bevezetése lehetővé

teszi a gyors és hatékony utazást és növeli a biztonságot is, mivel az egyedi ujjlenyomatok alkalmazása csökkenti az utazók személyazonosságával kapcsolatos kockázatokat. Chicagóban bizonyos benzinkutakon már ujjnyomattal is fizethetnek, az ujjnyomat érzékelős készülékek az autósok bankszámlájához kapcsolódnak, így a fizetés onnan történik. Japánban pedig ujjnyomat érzékelős pénz automatákat alkalmaznak bizonyos bankok ATM rendszerei, pénzfelvétel céljára [3].

2.3. Írisz azonosítás

Az írisz alapú azonosítás egy innovatív biometrikus technológia, amely az azonosítást az írisz egyedi mintázatainak elemzésével végzi. Az írisz nem más, mint a szem színes, gömb alakú része, amely rendkívül egyedi és stabil biometrikus jellemzőket tartalmaz, amik segítségével kitűnően alkalmas azonosításra.

A szem szivárványhártyájának mintázatán körülbelül 400 azonosítási jellemző található, így ez a biometrikus azonosítás a legjobb módszerek közé tartozik. Az írisz az embrionális fejlődés 8. hónapjáig alakul ki és annak az esélye, hogy két írisz megegyezzen $1:10^{70}$ a valószínűsége, tehát mondhatjuk, hogy közel lehetetlen [6]. Kialakulása után csak nagyon radikális esetekben változik. Ilyenek lehetnek például a szürkehályog, közvetlenül a szemet, illetve a fejet érintő balesetek, valamilyen kémiai anyag kihatása, vagy a szemet érintő műtétek.

A vizsgálat során a szivárványhártya látható és láthatatlan tulajdonságait elemzik. Az előbbi közé tartozik az írisz sugaras mintázata, a körökkel, árkokkal és a koronával. Utóbbi esetén pedig az infravörös leolvasás segítségével láthatóvá váló retinahártya ereket [3]. Az infravörös fényvel történő leolvasásnak köszönhetően éjszaka vagy alacsony fényviszonyok között is hatékonyan detektálhatók egyedi személyazonosító jegyek.

Az azonosítandó szempontjából két féle rendszert különböztetünk meg: aktív és passzív. A különbséget a felhasználó közreműködésének a szükségessége teszi. Az aktív leolvasási eljárások esetében a szemnek 15-35 cm-re kell elhelyezkednie a kamerától, a passzív módnál ezzel szemben elég 30-100 cm távolság a leolvasáshoz. Passzív eljárás esetén több kamera segítségével történik a vizsgálat, az elsődleges nagy látószögű kamera

meghatározza a szem helyzetét, a másodlagos kamera ráfókuszál a szemre és elvégzi az írisz leolvasását [6]. Az eltérő távolsági követelmények mellett mindkét módszernek megvannak az előnyei. Az aktív leolvasásnál a közeli távolság lehetővé teszi a részletes és precíz információgyűjtést ezzel növelve a pontosságot, míg a passzív módszer alkalmazása szélesebb körben megvalósítható, és könnyen integrálható olyan rendszerekbe, ahol a szem és a kamera közötti távolság változhat.

A kapott paramétereket 256 byte méretű kóddá, az ellenőrzés adatait ugyancsak 256 byte-os kóddá konvertálja az eszköz. Az azonosítás során az aktuális mintát összehasonlítja az adatbázisban található mintákkal [5]. Ezek alapján könnyen számolhatunk mekkora méretű tárterületre lesz szükségünk, amennyiben ezt a módszert szeretnénk használni. Evvel egyidejűleg a rendszer költségességébe is némi betekintést kaphatunk.

Az íriszfelvétel során egyéb tulajdonságokat is vizsgálnak, például átmérőt, elhelyezkedést vagy a pupilla pulzálását. Így csökkenthető a kontaktlencsével történő visszaélések valószínűsége [6]. Az így kapott többletinformációk nem csak a csalókkal szemben hasznosak, hanem abban az esetben is, ha valaki a kontaktlencsék, mint szemészeti segédeszközt hordja, mivel azok is jelentős mértékben módosíthatják az írisz megjelenését. Hasonlóképpen befolyásolhatja a vizsgálat eredményét, mint az arc alapú azonosítás során a smink viselése.

Az írisz azonosításon alapuló technika nagy hátránya, hogy a berendezések rendkívül bonyolultak, így áruk is magas [3]. Ez talán az egyik legnagyobb hátránya a többi rendszerrel szemben, ami azt is eredményezheti, hogy kevésbé lesz elterjedt a mindennapi használatban. Ugyan ez az azonosítási folyamat rohamosan fejlődik és egyre elterjedtebb, 2015-ben már mobiltelefonokban (ZTE Grand S3, Vivo X5Pro) is elérhető volt [6]. Azonban a mai trendeket figyelembe véve a telefonokban már nem igazán lelhető fel ez az azonosítási lehetőség az ujjlenyomat és az arc alapú azonosítással ellentétben. Ezen kényelmes és gyors azonosítási módok népszerűsége azt mutatja, hogy a felhasználók egyre inkább elvárják a magas szintű kényelmet és könnyű használhatóságot az eszközeikkel szemben. Az ujjlenyomat-alapú és az arc alapú azonosítások a modern mobiltelefonok elterjedt funkcióivá váltak, amelyek hatékonyan ötvözik a biztonságot és a felhasználói kényelmet a mindennapi használat során.

2.4. Retina azonosítás

A retina egy vékony, fényérzékeny réteg a szem hátulsó részén, amely az erek és idegek összetett hálózatát tartalmazza.

Az írisz a retinaazonosítással szemben több szempontból is előnyt élvez. A retina változhat cukorbetegség, drogok, vagy nagyobb mennyiségű alkohol fogyasztása esetén [5]. Hiába pontosabb tehát az íriszrel vagy akár más biometrikus azonosításokkal szemben, könnyebben elváltoztatható, ami sok problémát vethet fel, vagy éppen bizonyos helyeken és esetekben el is lehetetlenítheti a mindennapokban történő rendszeres használatát.

A működése azon alapszik, hogy az infrasarkanak eltérő mértékben nyelődnek el a vér oxigéntartalma miatt, evvel kirajzolva a szemfenék érhálózatát [3]. Hasonlóképpen amikor a kéz vagy az ujjvégek esetén történik az érrendszer feltérképezése.

A módszer egyik legnagyobb hátrányát az jelenti, hogy a mintavételezési eljárás során az olvasóval közvetlen kapcsolatot kell kialakítania a szemnek, ami által nő a fertőzésveszély [3]. Ez kihívások elé állíthatja a rendszerek tervezőit és üzemeltetőit a felhasználók egészségvédelme szempontjából a rendszer közösségi térben vagy tömegközlekedési eszközökön történő használata esetén. Annak érdekében tehát, hogy a retina alapú azonosítás elterjedhessen, fontos fejlesztések szükségesek a technológia higiéniai és egészségügyi vonatkozásaiban.

A szem hátsó falán futó érhálózat képe a halál beálltával megváltozik, és nem távolítható el a szervezetből, vagyis ellopása lehetetlen [2]. Ez komoly tényező a rendszer biztonságosságát tekintve. Ebből is kifolyólag a retina alapú azonosítás alkalmazása leginkább magas biztonsági követelményeket igénylő helyeken gyakoribb. Ilyenek lehetnek például katonai létesítményekben vagy kormányzati intézményekben, valamint bizonyos iparágakban és kutatási területeken.

3. EMPIRIKUS KUTATÁS

A kutatásom során kiemelten fontosnak tartottam az anonim módszertan alkalmazását az empirikus, vagy más néven tapasztalati kutatás keretein belül. A szisztematikusan tervezett vizsgálat során az anonimitás biztosítása volt az egyik prioritásom, mivel ennek révén lehetőséget teremtettem arra, hogy a résztvevők adatai teljes bizalmasságban kezelhetők legyenek.

A kutatás kvantitatív szemléletmódját választva a megbízható és objektív eredmények elérése volt a célom. A mérhető adatok és statisztikai elemzések segítségével nem csak mélyebb betekintést nyertem a kutatás témájába, hanem biztosítottam is azt, hogy az eredmények validak legyenek. Az anonim módszertan alkalmazása továbbá hozzájárult a résztvevők bizalmának növeléséhez, mivel garantáltam számukra, hogy személyes adataik védelme érdekében minden szükséges intézkedést megtettem.

A kutatás során részt vevő egyénnel folytatott interakcióim részeként, számos különböző témát érintő kérdéseket tettem fel, melyek célja az volt, hogy alaposan megvizsgáljam a biometrikus azonosítás különböző aspektusait. Az általam feltett kérdések egyik fő fókuszja az elfogadottság volt, melynek kapcsán arra kerestem választ, hogy a résztvevők mennyire hajlandóak elfogadni és alkalmazni ezt a technológiát a mindennapi életük során. A másik fontos terület, amelyet megvizsgáltam, a biztonságára vonatkozott. A kérdések ezen a téren arra irányultak, hogy milyen mértékben bíznak a résztvevők abban, hogy a biometrikus azonosítás hatékonyan védi személyes adataikat és információikat. A biztonsági aggályok és a bizalmatlanság ezen a területen jelentős hatással lehetnek a technológia elfogadására, így fontos volt, hogy részletesen megvizsgáljam ezt a szempontot is. Ezenkívül a kutatás során olyan kérdésekkel is foglalkoztam, amelyek a biometrikus azonosítással történő és a hagyományos fizetési módok közötti preferenciákat célozták meg. Ezen kérdések révén szerettem volna feltérképezni, hogy a résztvevők milyen mértékben részesítik előnyben a biometrikus azonosítás általi fizetést a hagyományos módszerekkel szemben. Mindezek az érdeklődési területek és a hozzájuk kapcsolódó kérdések részletes betekintést nyújtanak a kutatásba, és segítenek abban, hogy a biometrikus azonosítás elfogadottságát és alkalmazását alaposan megértsük a résztvevők szemszögéből.

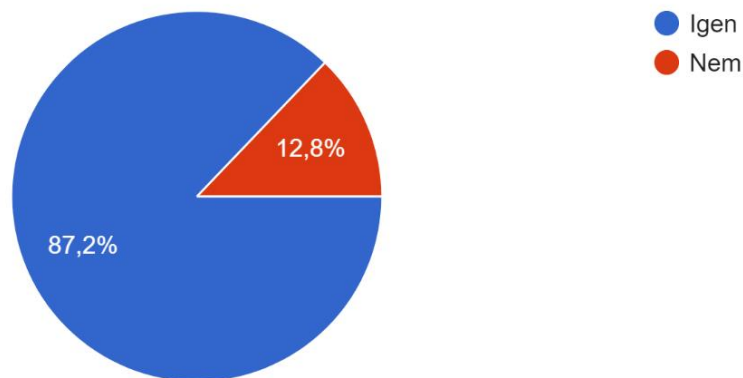
A kutatásban összesen 109 résztvevő vett részt anonim módon, akiket a részletes demográfiai elemzés érdekében különböző generációkba csoportosítottam. A résztvevők eloszlását részletesen rögzítettem a második táblázatban, amely szemlélteti, hogy a kutatásban hány főt sorakoztatnak az egyes generációk.

Generáció	Kitöltők száma
Z generáció	86
Y generáció	12
X generáció	11

2. táblázat: A kérdőív kitöltőinek generáció szerinti eloszlása

A táblázat alapján világossá válik, hogy a 109 fős minta tagjainak többsége a Z generációba sorolható. Az említett táblázat átlátható és követhető módon prezentálja a kutatás résztvevőinek generációs megoszlását, lehetővé téve a kutatók és az érdeklődők számára, hogy könnyen áttekinthessék a kiválasztott minta demográfiai összetételét. Ebben a szemléletes ábrázolásban a generációs kategóriák elrendezése és az egyes generációkhoz tartozó résztvevők számának feltüntetése segít a kutatás eredményeinek jobb értelmezésében, különös tekintettel a generáció-specifikus mintázatokra és véleményekre.

A vizsgálat előtt érdemes megfigyelni továbbá, hogy a résztvevők közül hányan használnak már most is valamilyen formában biometrikus azonítást, akár a telefonjuk feloldásához, vagy éppen netbankjukhoz történő bejelentkezéshez és online vásárlásnál a tranzakciók megerősítéséhez. Ezt az eloszlást a következő, egyben a harmadik, ábra illusztrálja:



3. ábra: A már valahol biometrikus azonosítást használók aránya

Az ábra részletes elemzése azt mutatja, hogy a kutatásban részt vevő egyének túlnyomó többsége már rendelkezik tapasztalattal a technológia különböző területein való használatában. Az előző technológiai tapasztalatok birtoklása segítheti a résztvevőket abban, hogy könnyebben alkalmazkodjanak és megszokják az új technológiai megoldásokat más területeken is. Ez a fajta széleskörű technológiai alkalmazkodásra való hajlandóság azt sugallja, hogy a résztvevők valószínűleg kevésbé zárkóznak majd el más, esetlegesen számukra kevésbé ismert területek technológiai megoldásai elől a jövőben. Ennek következtében az ábrán bemutatott pozitív tapasztalati háttér későbbi befolyásoló tényező lehet a technológia elfogadásának terén.

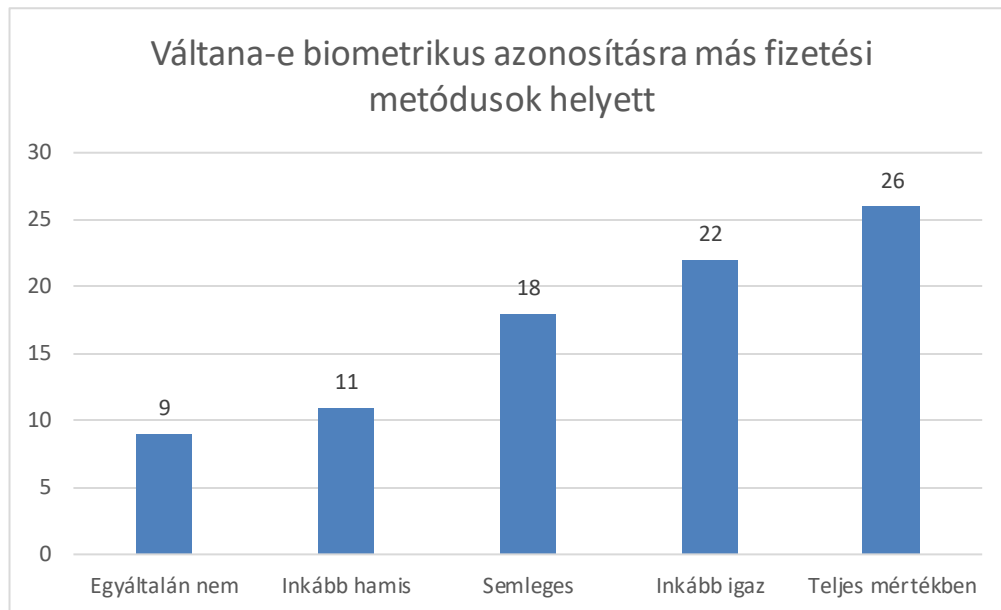
I Hipotézis

Feltételezhetően a Z generáció többsége elfogadóbb lenne a biometrikus azonosítással történő fizetéssel.

A hipotézis arra utal, hogy a Z generáció valószínűleg nyitottabb és elfogadóbb a biometrikus azonosításon alapuló fizetési módszerek iránt. Ennek a generációnak a tagjai, a digitális technológiák térhódítása idején nőttek fel, így valószínűleg könnyebben fogadják el a modern technológiákat az élet különböző területein. Úgy vélhetik, hogy a biometrikus azonosítás, például az ujjlenyomat- vagy arcfelismerés, számukra természetes és hatékony módja lehet a fizetési tranzakciók elvégzésének, egyszerűsítve

és felgyorsítva azokat a hagyományos fizetési módokhoz képest. Az elfogadottságuk megértése fontos szerepet játszhat a pénzügyi szolgáltatóknak és kereskedőknek, akik alkalmazkodni szeretnének az új generáció preferenciáihoz és elvárásaihoz.

A kérdőívem során megkérdeztem a kitöltőket, hogy mennyire értenek egyet avval az állítással, hogy szívesen váltanának-e valamely biometrikus azonosítási módszerre az eddig általuk használt fizetési metódusokról. A válaszokat a negyedik ábra szemlélteti:



4. ábra: Z generáció biometrikus azonosításra váltásra való hajlandósága

Ahogy a diagramban is jól megfigyelhető a válaszadók 56%-a, azaz valamennyivel több mint a fele szívesen élne a lehetőséggel. Evvel szemben mindössze 23% mondta, hogy inkább maradna a bankkártyás tranzakciónál. 21% semleges maradt a kérdést illetően, tehát ők ugyanannyira meg vannak elégedve a jelenleg használt módszerrel és nem látnak különösebb indokot a váltásra, hogy más fizetési metódust használjanak. Valószínűleg hasonló kényelmet és gyorsaságot társítanak a jelenlegi fizetési procedúrájuknak és a biometrikus azonosítással történő fizetésnek. Elképzelhető, hogy esetükben a biztonság nem játszik nagy szerepet, vagy meg vannak elégedve a jelenlegi fizetési módszerük biztonságával. A váltás támogatói viszont a semlegeseket figyelmen kívül hagyva több mint kétszer annyian voltak.

Az egyre növekvő hajlandóság a biometrikus azonosítási módszerek, például ujjlenyomat- vagy arcfelismerés iránt, részben a már meglévő tapasztalatokból is eredhet, amelyeket a felhasználók más szolgáltatások használata során szereztek. Amennyiben egy egyén már korábban találkozott és sikeresen alkalmazott biometrikus azonosítási technológiával egy másik környezetben vagy szolgáltatásnál, abban az esetben ez a pozitív élmény hatással lehet a hozzáállására és elfogadására a jövőbeni hasonló technológiákkal szemben. Ez az előző tapasztalat alapján kialakult bizalom erősítheti a biometrikus azonosítási módszerek elfogadását, és növelheti az emberek nyitottságát az ilyen típusú technológiák iránt más alkalmazásokban vagy szolgáltatásokban. Ennek következtében az egyszer már bevált biometrikus megoldások elterjedésére lehet számítani, miközben a technológiai innováció és elfogadás terén továbbra is folyamatos fejlődés tapasztalható.

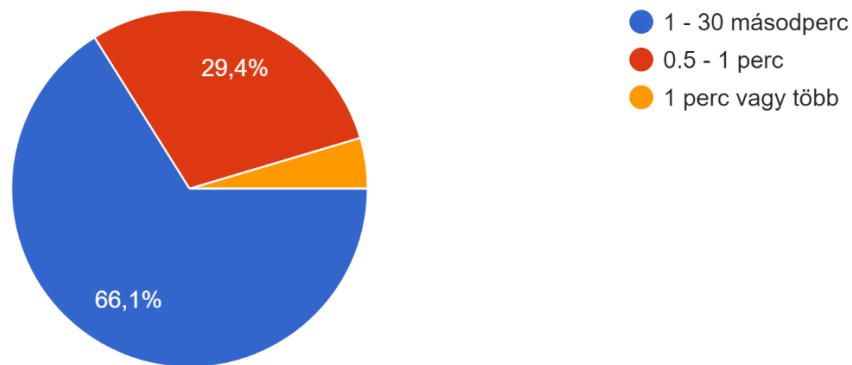
Az eredmény alapján megállapítható, hogy a Z generáció jelentős része pozitívan fogadja a biometrikus azonosítással történő fizetési módra való váltást. Az elfogadottság meghaladja az általános elfogadási arányt, ami azt sugallja, hogy a biometrikus fizetési megoldásoknak jelentős potenciáljuk lehet a fiatal generáció körében. A hipotézis tehát elfogadható.

II Hipotézis

Feltételezhetően a biometrikus azonosítás gyorsabbá teheti a fizetési tranzakciókat, mivel nem szükséges hosszú PIN-kódot vagy jelszót beírni.

A kutatás középpontjában a biometrikus azonosítás hatása áll a fizetési tranzakciók sebességére. Azt feltételezzük, hogy a biometrikus azonosítás, mint például ujjlenyomat- vagy arcfelismerés használata, lehetőséget teremt a felhasználók számára, hogy gyorsabban és hatékonyabban azonosítsák magukat a fizetés során, ezzel minimalizálva a tranzakciók időtartamát. Jelentősen csökkenthető lenne a fizetési időtartam kihagyva azokat az időigényes lépéseket, mint a hosszú PIN-kódok, jelszavak beírása, vagy online fizetés esetén kártyánkat használva a bankunk telefonos applikációjában szükséges megerősítés.

A kutatás során felmértem, hogy az emberek átlagosan mennyi időt töltenek fizetéssel. Ebbe egyaránt beletartoznak a készpénzzel fizetők és a bankkártyát használók is. Mindkét esetben megvannak a folyamatot lassító tényezők. A készpénz esetén például a visszajáró számolása, bankkártya esetén a PIN kód lassíthatja a folyamatot, aminek a következtében a biometrikus azonosítás gyorsabb megoldásnak bizonyulhat. A kitöltők megoszlását az alábbi ötödik ábra illusztrálja:



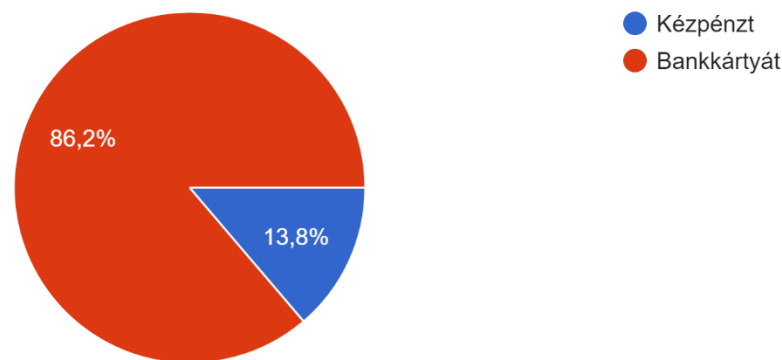
5. ábra: A megkérdezettek tranzakció idejüknek hossza

Az adatok elemzése során feltártuk, hogy a végrehajtott fizetési tranzakciók jelentős része, konkrétan a 66%, rendkívül gyorsan, fél perc alatt lezárult. Ezen kívül észleltük, hogy a tranzakciók 30%-a fél és egy perc közötti idő alatt zajlott le, míg az esetek kis hányada, mindössze 4%, meghaladta az egy percet. Ezen eredmények alapján arra lehet következtetni, hogy a biometrikus azonosítás alkalmazása nem feltétlenül járul hozzá a fizetési tranzakciók gyorsaságának növekedéséhez. Fontos megjegyezni ugyan, hogy a tranzakciók ideje változó lehet attól függően, hogy milyen biometrikus azonosítási módszert alkalmaznak, valamint a rendszer és a technológiai környezet egyedi jellemzőitől.

Feltehetően ennek az lehet az oka, hogy rendkívül elterjedt és széleskörben használatos bankkártyák esetén az NFC segítségével történő fizetés, aminél elegendő odaérintenünk a kártyánkat a terminálhoz a tranzakció végbemeneteléhez. Ez hasonlóan csak néhány másodpercet vesz igénybe, mint a biometrikus azonosítás. Mindemellett nem minden esetben szükséges a PIN kód használata. Ez ugyan csökkenti a biztonságosságát, de

cserébe viszont minimalizálja a folyamathoz szükséges időt, így megközelítheti vagy be is érheti a biometrikus azonosítással történő fizetés gyorsaságát.

Az eredménynél érdemes kiemelni, hogy nem csak a bankkártyát használók, hanem a készpénzzel fizetők is beletartoztak a korábbi kimutatásba. A két módszer megoszlását a hatodik ábráról olvashatjuk le:



6. ábra: A készpénz és a bankkártya használatának eloszlása a kitöltők között

Az ábrán bemutatott eredmények körképét tekintve látható, hogy a megkérdezettek túlnyomó többsége preferálja a bankkártyát a mindennapi vásárlásaik során, és ezt a fizetési módot választja a készpénzes tranzakciókkal szembeni előnyei miatt. A bankkártyás fizetés dinamikus elterjedése az utóbbi években részben annak köszönhető, hogy rendkívül hatékony és gyors módja a pénzügyi tranzakcióknak, különösen a készpénzhasználattal szemben.

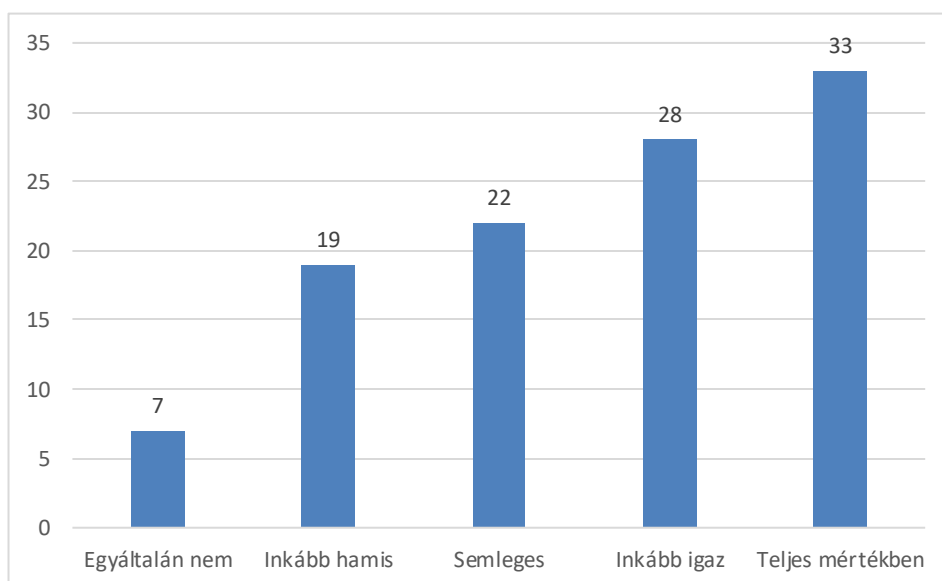
A kutatás eredményei alapján megállapítható, hogy a biometrikus azonosítással nem érhető el számottevően nagy mértékű gyorsítás a tranzakciók idejét tekintve a bankkártyákkal szemben, ezért a hipotézist el kell utasítanunk.

III Hipotézis

Feltételezhetően növelhető lenne a vásárlási élmény a biometrikus bankkártya rutinszerű alkalmazása által, mivel az kényelmesebb és hatékonyabb azonosítást tesz lehetővé.

A hipotézis alapján a rendszeres biometrikus bankkártyahasználat valószínűsíthetően elősegítené a vásárlási élmény fokozását, mivel ez a megközelítés kényelmesebb és hatékonyabb azonosítást tesz lehetővé. A hagyományos bankkártyák alkalmazásával járó PIN-kód beírás vagy aláírás gyakran időigényes és kellemetlenné válhat. A biometrikus azonosítás, mint például az ujjlenyomat- vagy arcfelismerés alkalmazása, lehetővé teszi a felhasználóknak, hogy gyorsan és egyszerűen azonosítsák magukat, ezáltal fokozva a fizetési folyamat hatékonyságát és kényelmét. Ez a változás nemcsak a tranzakciók sebességét növelheti, hanem pozitív hatással lehet a vásárlói élményre is, csökkentve a várakozási időt és javítva az üzletekben vagy online vásárlások során tapasztalt egyszerűséget.

A kérdőívben megkérdeztem a részt vevőket, hogy mennyire értenek egyet avval az állítással, hogy a biometrikus azonosítással történő fizetés kényelmesebb a bankkártyával, vagy egyéb lehetőségekkel szemben. A kapott válaszokat a hetedik ábra szemlélteti:



7. ábra: A biometrikus azonosítás kényelmessége a kitöltők szerint

A fenti diagram elemzése során azt tapasztalhatjuk, hogy a résztvevők 61%-a kényelmesebbnek ítélné meg a biometrikus azonosítást, míg 22% mondta, hogy nem lenne sem kényelmesebb sem kényelmetlenebb áttérnie, és 26% kényelmetlenebbnek ítélte a használatát. Ezek az eredmények megerősítik a hipotézis első részét, amely szerint a biometrikus azonosítás növelheti a vásárlási élményt a kényelmes és hatékony azonosítás révén.

A kényelmesség során több tényező is közre játszhat, ami egyénekenként eltérő lehet. Ilyen igények lehetnek a gyorsaság, megbízhatóság, magának a módszernek a folyamata, valamint az is befolyásolhatja a biometrikus azonosítás kényelmi aspektusát, hogy nem szükséges magunknál tartunk semmit, nem tudjuk otthon felejtetni, vagy amennyiben valamilyen megoldás által a telefonunk segítségével fizetünk nem kell tartanunk attól, hogy az akkumulátorunk időközben lemerül és fizetéseképtelenek leszünk.

A kutatás eredményei tehát azt sugallják, hogy a biometrikus bankkártyák rutinszerű alkalmazása nagyobb részben kényelmes és hatékony azonosítást eredményez, ami hozzájárul a vásárlási élmény pozitív irányú változásához, így a hipotézist elfogadhatjuk.

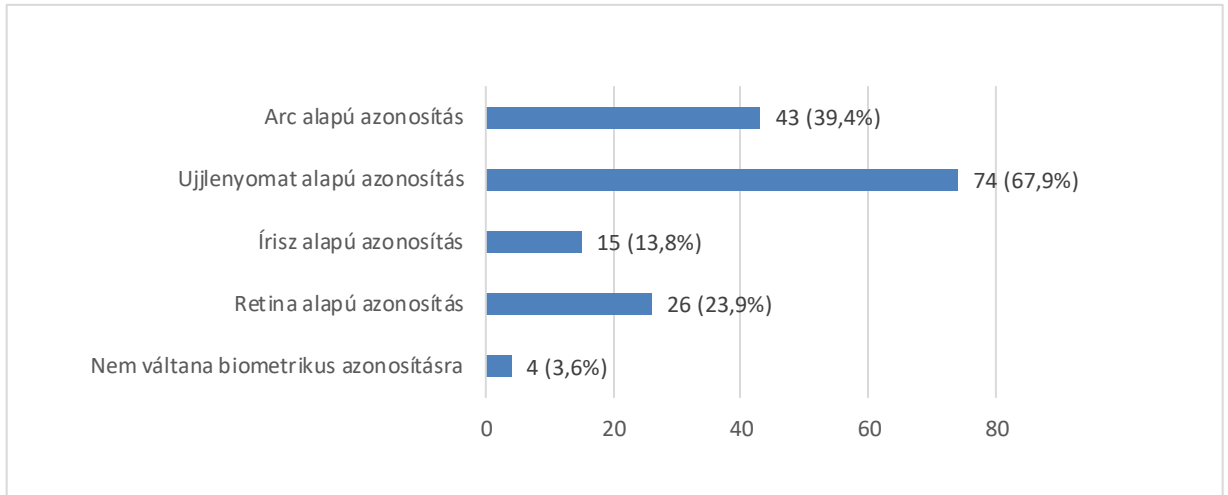
IV Hipotézis

Feltételezhetően a biometrikus azonosítási lehetőségek közül az ujjlenyomat azonosítást választaná a legtöbb ember a bankkártya kiváltására.

E hipotézis mögött az a feltevés áll, hogy az ujjlenyomatok egyedi és stabil jellemzői, valamint az ezen alapuló technológia elterjedtsége, kényelme és megbízhatósága együttesen teszik azt a legvonzóbb biometrikus azonosítási opcióvá a felhasználók számára.

A kutatásban résztvevők aktív részvételével végzett elemzés kiemelkedő jelentőségű volt annak érdekében, hogy feltérképezzük, mely biometrikus azonosítási módszerekre váltanának a jövőben szívesen a felhasználók. Fontos hangsúlyozni, hogy a résztvevőknek lehetőségük volt több általuk preferált biometrikus azonosítási módszer

megjelölésére, ha úgy gondolták, hogy több technológia is hatékonyan kiszolgálhatja szükségleteiket. A kutatás során kiderült, hogy a biometrikus azonosítási módszerek elterjedtsége és elfogadottsága számos tényezőtől függ, és a résztvevők preferenciái széles skálán mozognak, amit az alábbi nyolcadik ábra is szemléltet:

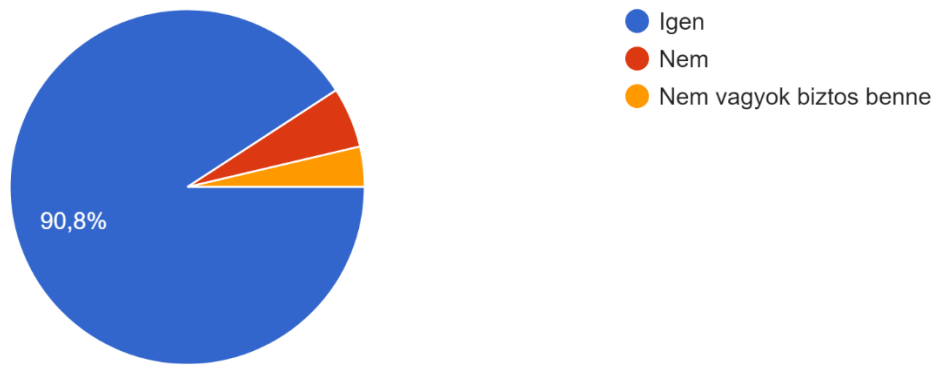


8. ábra: Biometrikus azonosítási preferenciák.

Az ábra azt mutatja, hogy a résztvevők körében az ujjlenyomat-azonosítás 67%-os elfogadottsággal kiemelkedően magas népszerűségnek örvend. Ez a technológia hatékony és megbízható biometrikus azonosítási módszerként tűnik fel, ami magyarázhatja népszerűségét a felhasználók körében. Emellett más biometrikus módszerek, például az arcazonosítás (40%), retina- (24%) vagy irisszkenner (13%) is számottevő támogatottságot élveznek, bár az egyéni preferenciák és kényelmi szempontok alapján jelentős különbségek mutatkoznak a válaszadók között.

Az elterjedtség, könnyű használat és megbízhatóság különféle biometrikus azonosítási technológiák esetében kulcsfontosságú tényezők, amelyek hozzájárulnak a felhasználók nyitottságához és elfogadásához. Az ujjlenyomat- és az arc alapú azonosítás kiemelkedik a mindennapokban legelterjedtebb biometrikus azonosítási módszerek közül. Ezek a technológiák már széles körben elterjedtek, különösen a mobiltelefonok terén. Az, hogy ezek a megoldások könnyen hozzáférhetőek és beépítve vannak a legtöbb telefonba, elősegíti az elterjedésüket és magyarázatot ad arra, hogy miért válnak oly népszerűvé.

A kérdőívemben fel is tettem a kérdést, miszerint rendelkezik-e a kitöltő által használt mobiltelefon valamilyen biometrikus azonosítási funkcióval, legyen az akár ujjlenyomat vagy arc alapú azonosítás. A kapott eredmény szerinti eloszlást a kilencedik ábra szemlélteti:



9. ábra: Rendelkezik-e biometrikus azonosításra képes telefonnal

Az ábrán egyértelműen látszik, hogy a megkérdezettek elsöprő többségének mobilja rendelkezik ilyen funkcióval, így nem meglepő, hogy a telefonokban alkalmazott két legnépszerűbb biometrikus azonosító örvend a legnagyobb népszerűségnek.

Befolyásoló tényező lehet továbbá a módszer használatának kényelmessége. A mindennapokban talán az egyik legkényelmesebb módszer az arc alapú azonosítás, mivel az a megoldás működik a leginkább passzív helyzetben is, hogy az embernek ne kelljen semmit csinálnia. A második az ujjlenyomat olvasás, mivel ott elegendő odahelyeznünk az ujjunkat az érzékelőre és már készen is van. Ezekkel szemben az írisz és a retina alapú azonosítás kicsivel több közreműködést igényel, mint az előbb említett két rendszer, mivel itt oda kell hajolni a kamerához, hogy az azonosítani tudjon minket. Sőt a retina alapú azonosítás esetében még fizikai kapcsolat is szükséges a szemünk és az érzékelő között, ami nem csak kényelmetlen, de rendkívül bonyolult lenne a megvalósítása a higiénia szempontjából például tömegközlekedésen való fizetés esetében.

A kutatás eredményei alapján elmondható, hogy az ujjlenyomat alapú biometrikus azonosítás kiemelkedően népszerű a felhasználók körében. Ebből kifolyólag tehát elfogadható a korábban támasztott hipotézis.

4. HIPOTÉZISEK IGAZOLSÁSA, ELVETÉSE

A kutatás egyöntetűen azt támasztja alá, hogy a biometrikus azonosítást a bankkártyák kiváltására vonatkozóan kiemelkedő elfogadottsággal és elégedettséggel fogadják a fiatalabb generáció körében. Az ujjlenyomat-azonosításnak kifejezetten pozitív megítélése volt. Ezen technológia kiemelkedő hatékonysággal és biztonságossággal szolgál a felhasználók számára, így pozitív irányú változásokat eredményezhet a későbbiekben a gyakorlati alkalmazást követően az eddig inkább elutasító felhasználók körében is.

A biometrikus azonosítás sikerességében hozzájáruló tényezők közé tartozik a rendkívül hatékony ujjlenyomat-azonosítási technológia, amely a felhasználók részéről kiváló elégedettséget váltott ki. Az ujjlenyomatok egyedülálló biometrikus jellemzőként szolgálnak, amelyek szinte azonnali és megbízható azonosítást tesznek lehetővé, jelentősen felülmúlva a hagyományos jelszavak vagy PIN-kódok használatát. Ez a fajta hatékonyság kivételes kényelmet biztosít a felhasználóknak, akiknek csupán egy egyszerű érintésre van szükségük a tranzakciók hitelesítéséhez.

A biztonság iránti növekvő igény és az ujjlenyomat-azonosítás megbízhatóságának meggyőző eredményei együttesen segítik elő a biometrikus azonosítás iránti pozitív fogadtatást. Az ilyen technológiák által biztosított magas szintű védelem és a felhasználói adatok intimebb biztonsága jelentős előnyökkel jár, különösen, amikor a pénzügyi tranzakciók és az érzékeny adatok kezelése a központi kérdések egyike. A felhasználók pozitív élményei és elégedettsége tovább erősíti a biometrikus azonosítás iránti keresletet, így elkerülhetetlenül előmozdítva az ezen technológiák által inspirált innovációkat és fejlesztéseket a pénzügyi szektorban.

Hipotézis	Elfogadás/Elutasítás
Feltételezhetően a Z generáció többsége elfogadóbb lenne a biometrikus azonosítással történő fizetéssel.	A korábban bemutatott eredmények alapján a hipotézist elfogadhatjuk.
Feltételezhetően növelhető lenne a vásárlási élmény a biometrikus bankkártya rutinszerű alkalmazása által, mivel az kényelmesebb és hatékonyabb azonosítást tesz lehetővé.	A fentebbi vizsgálat alapján a hipotézist elfogadhatjuk.
Feltételezhetően a biometrikus azonosítás gyorsabbá teheti a fizetési tranzakciókat, mivel nem szükséges hosszú PIN-kódot vagy jelszót beírni.	A kutatás eredményei alapján a hipotézist elutasíthatjuk.
Feltételezhetően a biometrikus azonosítási lehetőségek közül az ujjlenyomat azonosítást választaná a legtöbb ember a bankkártya kiváltására.	A korábbi eredmények alapján a hipotézist elfogadhatjuk.

3. táblázat: Hipotézisek összesítése.

5. BANKKÁRTYÁK KIVÁLTÁSA BIOMETRIKUS AZONOSÍTÁSSAL A GYAKORLATBAN

5.1. Hol használható fel a kutatás eredménye

Az előzőleg vizsgált négy hipotézis eredményei számos területen kínálnak alkalmazási lehetőségeket, ahol a biometrikus azonosítások innovatív és hatékony megoldást jelenthetnek. Nem csupán a bank szektorban használható fel, hanem akár az egészségügyben vagy vállalatok esetében is.

Az biometrikus azonosításnak széles körű alkalmazási lehetőségei vannak a pénzügyi területen. A bankok, pénzügyintézetek és egyéb pénzügyi szolgáltatók számára ez az eredmény lehetőséget kínál az azonosítás folyamatának egyszerűsítésére és gyorsítására. Az ATM-ek, banki alkalmazások és fizetési tranzakciók terén a biometrikus azonosítás segíthet a felhasználók számára kényelmesebb és biztonságosabb élmény kialakításában. Biztonság és megbízhatóság szempontjából a biometrikus azonosítás technológiai erősíti a személyazonosság biztonságát, mivel az ilyen egyéni jellemzők nehezen hamisíthatók és az validáláshoz az egyén fizikai jelenléte szükséges. A kényelmet tekintve a biometrikus azonosítás megkönnyíti és felgyorsíthatja a fizetési folyamatokat, minimalizálva a vásárlók időráfordítását. A biometrikus technológiák integrálása egy modern és innovatív megközelítést jelent, amely tovább növelheti egy bank vagy szolgáltató presztízsét.

A kiskereskedelmi területen való alkalmazása során az ujjlenyomat alapú azonosítás kiemelkedő lehetőségeket rejt magában az ügyfélszolgáltatások terén. Ezen technológia integrálása kiskereskedelmi hűségprogramokba vagy vásárlói kártyák kezelésébe lehetővé teszi a vásárlók számára például, hogy egyszerűen és gyorsan azonosítsák magukat, így élve az egyedi előnyökkel és kedvezményekkel.

Az egészségügyi intézmények számára az ujjlenyomat alapú azonosítás hasznos lehet a betegazonosításban és a kórházi rendszerekben. Ezáltal növelheti az adatbiztonságot, csökkentheti az esetleges hibákat, és egyszerűsítheti az egészségügyi szolgáltatások igénybevételét. Természetesen a használhatósága a sérüléstől függ, ugyanis például arc

alapú azonosítás esetén egy orrtöréssel jött beteget a rendszer nem lesz képes felismerni. Az egészségügyben indokolt lenne több módszert is alkalmazni egymás alternatívájaként.

A vállalati környezetben a biometrikus azonosítás előnyös lehet az épületek beléptetésében és az üzleti rendszerekhez való hozzáférésben. Ezenkívül az IT biztonsági intézkedések részeként is alkalmazható, így a vállalatok hatékonyabban védelmezhetik érzékeny információikat.

5.2. Javaslatok

A pénzügyi szolgáltatások területén az innováció és a technológiai fejlődés lehetőséget teremt arra, hogy a hagyományos bankkártyákat korszerűbb és biztonságosabb biometrikus azonosítási módszerekre válthassuk. Jelen javaslatok célja, hogy körvonalazza, hogyan lehetne hatékonyan integrálni ezeket az azonosítási módszereket a fizetési folyamatokba, felváltva ezzel a fizikai bankkártyák használatát.

Melyik rendszert érdemes használni?

A kutatásunk alapján arra a következtetésre jutottunk, hogy az ujjlenyomat-azonosítás rendkívül magas elfogadottsággal és megbízhatósággal rendelkezik a felhasználók körében. Ezen eredmények fényében ésszerű és előremutató javaslatként merül fel egy olyan rendszer kifejlesztése, amely lehetővé teszi az ujjlenyomat-azonosítás alapú fizetések széles körű alkalmazását.

Az ügyfelek edukálása az új rendszerre

A pénzügyintézetek számára kritikus feladatnak kell tekinteni a célcsoportoknak szóló részletes és célzott információs kampányok tervezését és végrehajtását, amelyek középpontjában a biometrikus azonosítási rendszerek előnyeinek és működésének ismertetése áll.

A sikeres tájékoztatási stratégiák kialakítása nem csupán egy új technológia megismertetését célozza, hanem egy olyan kultúraváltás elősegítését is, amelyben a felhasználók megértik és elfogadják a biometrikus azonosítás pozitív hatásait. Az információs kampányoknak részletesen be kell mutatniuk és kiemelniük ezen módszerek előnyeit, beleértve a rendkívüli biztonságot, a gyorsaságot és a felhasználóbarát felületeket. Emellett kellő hangsúlyt kell fektetniük a technológia működésének átlátható és érthető magyarázatára is, annak érdekében, hogy a felhasználók könnyen felfogják a folyamatot és megtapasztalják a biometrikus azonosítás egyszerűségét.

Az információs kampányok hatékonyságának növelése érdekében interaktív médiafelületek, élő demonstrációk és bemutatók alkalmazása is javasolt, hiszen ezek segíthetik a felhasználókat még közelebb hozni a biometrikus azonosítás mindennapi használatához, így hozzájárulva az elfogadási ráta erősítéséhez.

Összességében az információs kampányoknak egy átfogó, támogató és kézzelfogható keretet kell nyújtaniuk, amely meggyőzi a felhasználókat a biometrikus azonosítás értékéről és megbízhatóságáról.

Alternatív autentikációs módszerek használata biometrikus azonosítás mellett

A biometrikus azonosítás bevezetése során különös figyelmet kell fordítani az alternatív hitelesítési módszerek kialakítására és integrációjára.

Az alternatív módszerek nélkülözhetetlenek lehetnek olyan esetekben, amikor rendszerhibák vagy biometrikus adatok elérhetetlensége miatt az alapvető biometrikus azonosítás meghibásodik, vagy nem érhető el. Ezen alternatív autentikációs módszerek, mint például a PIN-kód vagy jelszó, szolgálhatnak biztonságos visszajárési pontként a rendszerhibák vagy technikai problémák idején. A felhasználók így képesek lehetnek más validációs eszközöket használni, hogy hozzáférjenek a pénzügyi rendszerhez vagy végezzenek tranzakciókat.

Ezenkívül az alternatív hitelesítési módszerek bevezetése nemcsak a rendszerműködés problémáinak esetén lehet kritikus, hanem szolgálhatnak azoknak a felhasználóknak is,

akik esetleg még nem kényelmesek vagy nem preferálják a biometrikus azonosítási módszereket. Az ilyen változatosság lehetőséget ad a felhasználóknak, hogy saját igényeiknek megfelelő verifikációs módszert válasszanak, ami növelheti az elfogadást és az elégedettséget.

Ez a rugalmasság segít fenntartani a pénzügyi rendszerek folyamatosságát és stabilitását még a váratlan események idején is. Az ilyen alternatív megoldások tervezése és implementálása része kell legyen a biometrikus azonosításba történő bevezetésnek, hogy biztosítsa a rendszer megbízhatóságát és felhasználóbarát működését a változatos körülmények között is.

Szigorú adatvédelmi intézkedések bevezetése

A bankkártyák biometrikus azonosítással történő kiváltása során kardinális fontosságú a rendszerbiztonság és az adatvédelem fejlesztése, valamint fenntartása. A pénzintézeteknek és technológiai vállalatoknak szorosán együtt kell működniük annak érdekében, hogy korszerű és megbízható rendszert hozzanak létre, amely védelmet nyújt a felhasználói adatoknak, különös tekintettel a biometrikus azonosításra alkalmazott adatokra. Az adatbiztonság terén a rendszerbiztonsági protokollok kiemelt figyelmet érdemelnek. A kifinomult biztonsági rendszerek, például a titkosított kapcsolatok, kétlépcsős hitelesítési eljárások és az esetleges támadások elleni védelmi mechanizmusok bevezetése nélkülözhetetlenek. A rendszerbiztonsági intézkedések célja, hogy megakadályozzák az illetéktelen hozzáférést, a csalásokat és a biztonsági réseket, ezáltal megerősítve a felhasználók bizalmát. Az adatvédelem terén kritikus fontosságú a magas szintű garanciák biztosítása a biometrikus adatok kezelése során. A felhasználókat részletesen tájékoztatni kell az ezeket érintő adatok gyűjtésének, tárolásának és feldolgozásának folyamatáról.

A technológiai fejlődés szoros kapcsolatban áll az adatbiztonság és adatvédelem kérdéseivel. Az esetleges fejlesztéseknél prioritást kell adni azoknak a mechanizmusoknak, amelyek megakadályozzák a biometrikus adatok jogosulatlan felhasználását vagy illetéktelen hozzáférését.

Rendszeres frissítések és ellenőrzések révén biztosítható, hogy a rendszer mindig a legmagasabb szintű biztonságot nyújtsa. Az adatbiztonság és adatvédelem megerősítése nem csupán technológiai kérdés, hanem egyúttal etikai és jogi megfontolásokat is magába foglal. Az ilyen komplex rendszerek tervezése és működtetése során a tervezőknek és üzemeltetőknek kiemelt figyelmet kell fordítaniuk azokra az értékekre és normákra, amelyek a felhasználói adatok tiszteletben tartását és védelmét szolgálják. Egy ilyen komplex megközelítés segíthet megőrizni a felhasználók bizalmát, ami kulcsfontosságú a biometrikus azonosítás elterjedésének és elfogadásának sikeres kivitelezéséhez.

Figyelemmel kell kísérni a jogi és szabályozási fejleményeket

A biometrikus azonosítás bevezetésekor kulcsfontosságú szempont az aktuális jogi és szabályozási környezet figyelemmel kísérése és a rendszer megfelelőségének biztosítása a vonatkozó adatvédelmi és szabályozási irányelvekkel szemben.

A jogi és szabályozási területeken bekövetkező változások és fejlemények nagy hatással lehetnek a biometrikus azonosítási rendszerek működésére és elfogadására, ezért kritikus fontosságú a folyamatosan frissülő szabályozási környezet követése. Az adatvédelmi előírásoknak való megfelelés érdekében azonosítási rendszerek tervezése és működtetése során fokozott figyelmet kell fordítani a személyes adatok védelmére és kezelésére vonatkozó szabályokra. A GDPR (Általános Adatvédelmi Rendelet) és hasonló adatvédelmi rendelkezések egyre növekvő jelentőséggel bírnak, és ezek betartása elengedhetetlen a felhasználók jogainak és magánéletének tiszteletben tartásához.

A jogi keretrendszer megfelelő követése mellett az is fontos, hogy a biometrikus azonosítás bevezetése során a bankok proaktívan együttműködjenek a hatóságokkal és az érintett szabályozó szervezetekkel. Ez a kommunikáció elősegíti, hogy a rendszerek megfeleljenek a legfrissebb iránymutatásoknak, és időben reagáljanak a változó jogi követelményekre.

A folyamatos együttműködés és a jogi keretrendszer alapos ismerete lehetővé teszi a pénzügyi intézmények számára, hogy fenntartsák a biometrikus azonosítás biztonságát és elfogadhatóságát, miközben biztosítják a felhasználók jogainak tiszteletben tartását.

Ennek révén a biometrikus azonosítás a jogi környezethez való alkalmazkodásával hozzájárulhat a modern és biztonságos pénzügyi technológiák fejlődéséhez és elterjedéséhez.

Felhasználókkal való megfelelő kommunikáció

A felhasználók aktív részvétele a biometrikus azonosítás rendszereinek tervezésében és fejlesztésében nem csupán jó gyakorlat, hanem kritikus fontosságú tényező a technológia sikeres bevezetése és elfogadása szempontjából.

A tervezési folyamatban való közvetlen bevonásuk révén a felhasználók egyedi nézőpontja, elvárásai és élményei előkerülnek, ami segít az innovációban és a technológiai alkalmazások hatékonyabb kialakításában. A rendszeres konzultációk és visszajelzési mechanizmusok bevezetése stratégiai lépés a fejlesztők számára. Az ilyen, rendszerességgel megtartott, konzultációk során a felhasználók szabadon megoszthatják gondolataikat, aggályaikat és igényeiket a tervezési folyamattal kapcsolatban. Ez a kölcsönös kommunikáció lehetővé teszi a fejlesztők számára, hogy a valós felhasználói szempontokon keresztül mélyebb megértést szerezzenek a technológia iránti igényekről és elvárásokról. A konzultációk során felmerülő visszajelzések értékes forrásokat jelentenek a folyamatok javításához és a rendszerek optimalizálásához. Az ilyen visszajelzések segíthetnek azonosítani a felhasználói elégedettségét növelő elemeket, valamint azokat a területeket, ahol további fejlesztések és finomhangolások szükségesek. A folyamatos visszacsatolás révén a rendszer könnyebben alkalmazkodhat a felhasználói igények változásaihoz és az új technológiai trendekhez.

Az elkötelezettség a felhasználók bevonása iránt nem csupán a tervezési folyamat kezdeti szakaszára korlátozódik. A rendszer üzemeltetése és a technológia életciklusának minden szakaszában kulcsfontosságú a folyamatos visszajelzési mechanizmusok és kommunikációs csatornák fenntartása. Ez lehetővé teszi a rendszer folyamatos alkalmazkodását az újabb felhasználói igényekhez és technológiai lehetőségekhez. A felhasználók aktív bevonása és a rendszeres konzultációk integrálása tehát egy átfogó és dinamikus folyamatot alkot, amely hozzájárul a biometrikus azonosítás technológiai

rendszerének hatékony és felhasználóbarát kialakításához. Ennek eredményeként a fejlesztőknek lehetőségük nyílik reagálni a felhasználói igények változásaira és fenntartani az elfogadást a szélesebb közönség körében.

Új technológiai infrastruktúra kialakítása

Az új technológiai infrastruktúra kialakítása és fejlesztése kiemelkedő jelentőséggel bír a biometrikus azonosítás sikeres bevezetésében, hiszen ez az alapköve annak, hogy a rendszer hatékonyan működhessen és megfeleljen a modern biztonsági és felhasználói elvárásoknak.

Ebben a folyamatban kiemelkedő szerepet játszanak a partnerségek, amelyek révén a szakértelem és erőforrások összevonásával még eredményesebben lehet elérni a kitűzött célokat. A partnerségek kialakítása lehetőséget teremt a különböző szervezetek, vállalatok és technológiai fejlesztők közötti együttműködésre. Az olyan partnerségek, amelyek összpontosítanak a biometrikus azonosítás fejlesztésére és alkalmazására, lehetővé teszik a tapasztalatok és szakértelem cseréjét. Mindezek mellett a különböző szereplők egyesített erőforrásai lehetővé teszik a technológiai infrastruktúra hatékonyabb kialakítását és optimalizálását.

A partnerségek nem csupán szinergikus előnyöket teremtenek, hanem lehetőséget kínálnak az innovációs projektek támogatására is. Az innováció kiemelt jelentőséggel bír a biometrikus azonosítás terén, mivel a technológia gyors fejlődése folyamatos újításokat követel meg. Az innovációs projektek lehetővé teszik a fejlesztők számára, hogy kísérletezzenek új megoldásokkal, technológiákkal és alkalmazásokkal, elősegítve ezzel a biometrikus azonosítás funkcionalitásának és megbízhatóságának folyamatos fejlődését.

Kompatibilitás biztosítása

A biometrikus azonosítási rendszerek tervezésekor és fejlesztésekor kardinális jelentőségű a kompatibilitás kérdése, különös tekintettel más pénzügyi rendszerekkel

és különböző eszközökkel való összeférhetőségre. A kompatibilitás azonban nem csupán technikai aspektusból fontos, hanem az egész pénzügyi ökoszisztémában való szoros integrációt és együttműködést is magában foglalja.

A rendszerek közötti együttműködés és információcsere képessége létfontosságú a biometrikus azonosítás terjedésének és elfogadásának szempontjából. Az olyan rendszerek, amelyek könnyen illeszthetők más pénzügyi platformokhoz, pénzforgalmi rendszerekhez vagy akár nemzetközi fizetési rendszerekhez, hozzájárulnak a szélesebb körű elfogadáshoz és alkalmazáshoz. Elősegíti a hatékonyabb és zökkenőmentesebb tranzakciókat különböző pénzügyi intézetek, bankok és fizetési szolgáltatók között. Ezenkívül megkönnyíti a felhasználóknak, hogy ugyanazt a biometrikus azonosítást használják többféle helyen és eszközön, például bankfiókokban, online vásárlások során vagy éppen mobilalkalmazásokban.

Ez a kompatibilitás nemcsak technikai szempontból, hanem szabályozási és jogi szempontból is fontos. A különböző pénzügyi és szabályozói rendszerek összehangolása lehetővé teszi, hogy a biometrikus azonosítás biztonságos és elfogadható módon működjön a különböző jogi környezetekben. Ezen túlmenően, az eszközök közötti kompatibilitás kiemelt szerepet játszik, különösen a mai sokféle okoseszköz és mobilplatformok korában.

A biometrikus azonosításnak alkalmazkodnia kell az olyan eszközök specifikációihoz, mint az okostelefonok, táblagépek, és akár az intelligens házak eszközei, hogy a felhasználók számára valódi kényelmet és rugalmasságot biztosítson. A széleskörű alkalmazhatóság és a zökkenőmentes integráció hozzájárul a biometrikus azonosítás globális térnyeréséhez és a pénzügyi szektor hatékonyabb működéséhez.

Kipróbálás kis környezetben

A biometrikus azonosítás bevezetése során javasolt lenne kis léptékű kísérletek és pilotprojektek alkalmazása, amelyeket kezdetben egy adott városban vagy egy meghatározott csoport körében lehet elindítani. Ez a lépésrend lehetőséget kínál a

rendszer alapos tesztelésére és a felhasználói visszajelzések gyűjtésére, mielőtt a technológia szélesebb körű elterjesztésre kerülne.

A kis léptékű kísérletek és pilotprojektek lehetővé teszik a fejlesztők és üzemeltetők számára, hogy a biometrikus azonosítás gyakorlati alkalmazásában tanuljanak a rendszer működéséről és az esetleges kihívásokról. Ez a próbaidőszak lehetőséget teremt a finomhangolásra és az esetleges hibák vagy hiányosságok kijavítására, mielőtt a rendszer szélesebb körben kerülne bevezetésre.

Mindezek mellett a rendszer teljesítményét és hatékonyságát is monitorozni lehet, ami különösen fontos a későbbi kiterjesztés során. A kezdeti tesztek alkalmával szerzett tapasztalatok segítenek optimalizálni a rendszert, és hozzájárulnak a stabil és megbízható működés kialakításához.

A visszajelzések begyűjtése lehetőséget teremt a felhasználók igényeinek és aggodalmainak figyelembevételére, így a rendszer fejlesztői képesek lesznek személyre szabni a technológiát a valós felhasználói elvárásoknak megfelelően. Ezek a kis léptékű kísérletek és pilotprojektek általában csökkentett kockázatot jelentenek a bevezetés kezdeti szakaszában, ezáltal a szervezetek és pénzüzetek fokozatosan és kontrollált módon ismerhetik meg és alkalmazhatják a biometrikus azonosítás előnyeit, mielőtt nagyobb léptékű implementációkba kezdenének.

Ujjlenyomat-azonosítás Bankautomatáknál

A javaslat szerint a pénzüzeteknek érdemes lenne integrálni az ujjlenyomat-azonosítást a bankautomaták funkcionalitásába. Ennek eredményeként a felhasználók a pénzügyi tranzakcióikat nem a hagyományos bankkártyák segítségével hajtánák végre, hanem egyszerűen és gyorsan azonosítanák magukat az ujjlenyomatuk révén.

Ez az innovatív megközelítés több szempontból is előnyös lehet. Először is, az ujjlenyomat-azonosítás rendkívül hatékony, mivel a felhasználók egyszerűen, pillanatok alatt hajthatnák végre tranzakcióikat. Másodszor, a biztonság szempontjából az ujjlenyomat-azonosítás rendkívül megbízható és a leginkább kedvelt azonosítási mód.

Ezenkívül az ilyen típusú fejlesztéseknek pozitív hatása lehet a felhasználói élményre is. A tranzakciók egyszerűségét és gyorsaságát figyelembe véve a felhasználók egyre inkább hajlamosak lehetnek elfogadni és alkalmazni az ujjlenyomat-azonosítást, ezáltal fokozva a digitális pénzügyi eszközök elfogadását.

Végül, az ilyen innovatív megoldások bevezetése a pénzügyi szolgáltatóknak lehetőséget ad arra, hogy a versenyképességüket növeljék, és vezető szerepet töltsenek be az iparágban. A modern technológia és a biometrikus azonosítások integrálása újabb lépés a pénzügyi szektor digitalizációjában, amely elősegítheti a biztonságos és hatékony pénzügyi tranzakciók elterjedését a globális piacon.

Finanszírozási támogatások keresése

Pénzintézetek és technológiai vállalatok esetében kiemelkedően fontos az innovációs projektek támogatása, különös tekintettel a biometrikus azonosítással kapcsolatos kutatásokra és fejlesztésekre. E projektek révén ugyanis ezek a szereplők nem csupán a saját technológiai előnyeiket növelhetik, hanem hozzájárulhatnak az ágazat szélesebb körű fejlődéséhez és a digitális biztonság további fokozásához.

Az ilyen típusú innovációs kezdeményezéseknek gyakran magas költségeik vannak, és a előnyös lehet különböző finanszírozási lehetőségek felkutatása. Az innovációs projektek finanszírozásának egyik lehetséges forrása az állami támogatások és pályázatok. A kormányzati szervek gyakran kínálnak támogatást az olyan kutatási és fejlesztési projektek számára, amelyek előrelépést jelentenek az adatbiztonság, a digitális azonosítás és a technológiai innováció területén. Ezek a támogatások nemcsak pénzügyi segítséget nyújthatnak, hanem elismerést is hozhatnak a projektek számára a szakmai és iparági körökben.

Egy másik lehetséges finanszírozási forrás a befektetők és kockázati tőke-alapok. Az olyan vállalkozások, amelyek a biometrikus azonosítás területén innovatív megoldásokat fejlesztenek magukhoz vonzhatnak befektetőket, akik hajlandóak tőkét biztosítani a projekt sikeres kivitelezéséhez. Az ilyen típusú partnerségek nemcsak pénzügyi

támogatást jelentenek, hanem az üzleti hálózatokat is bővíthetik, valamint szakmai tanácsadást és kapcsolatokat is hozhatnak a projektek mögé álló vállalatoknak.

A kormányi és magán finanszírozások mellett a nemzetközi támogatási alapok is lehetőséget kínálhatnak. Olyan szervezetek, mint az Európai Unió, számos programon keresztül támogatják az olyan projekteket, amelyek elősegítik a digitális innovációt és a biztonságos technológiák fejlesztését. A részvétel ezekben a programokban nemcsak finanszírozási forrásokat biztosíthat, hanem lehetőséget teremthet a projektek nemzetközi láthatóságára és együttműködésekre más szakértőkkel és vállalatokkal. Az ilyen típusú finanszírozási lehetőségek felkutatása és kihasználása lehetővé teszi a pénzügyi intézetek számára, hogy ambiciózus biometrikus azonosítási projekteken dolgozhassanak, amelyek előmozdítják az iparág fejlődését és innovációját. Ezenkívül ezek a támogatási források segíthetnek csökkenteni a fejlesztéssel járó kockázatokat, miközben hozzájárulnak a digitális biztonság és az azonosítási technológiák fejlesztéséhez a globális pénzügyi szektorban.

Ágazati együttműködések

Az új technológiai megoldások sikerének kulcsfontosságú aspektusa a bankok, kereskedők és technológiai szolgáltatók közötti szoros együttműködés. Az ilyen partnerségi kapcsolatok kiemelkedő jelentőségűek, mivel lehetővé teszik a különböző iparágakban tevékenykedő szereplők számára, hogy összefogjanak és közösen dolgozzanak azon, hogy a technológiai fejlesztések a lehető leghatékonyabban és összehangoltabban valósuljanak meg.

Az együttműködés elősegítheti a tudásmegosztást és az innovációt is. A pénzügyi intézetek, kereskedők és technológiai szolgáltatók közötti partnerségek során a felek gyakran megosztják egymással az iparági tapasztalataikat, legjobb gyakorlataikat és szakértelmüket. Ez lehetővé teszi, hogy a fejlesztések során kihasználják egymás erősségeit, és az innovációk gyorsabb ütemben valósuljanak meg.

Végül soron tehát a szoros együttműködés a bankok, kereskedők és technológiai szolgáltatók között alapvető tényező a sikeres technológiai megoldások bevezetésében.

A partnerségek révén létrejövő dinamikus együttműködés hozzájárul a hatékonyabb szabványok kialakításához és az új rendszerek optimális együttműködéséhez, elősegítve ezzel a digitális fejlődést és a pénzügyi szektor innovációját.

Szabványok kialakítása és betartása a biometrikus azonosítás területén.

A szabványok alapvető fontosságúak az új technológiai rendszerek széleskörű elfogadásához és integrációjához. A szabványok meghatározzák a rendszerek és alkalmazások közötti egységes kommunikációt és adatátvitelt, ezáltal biztosítva a kompatibilitást és az egységes működést. A közös szabványok kialakítása segíthet megelőzni a kompatibilitási problémákat, amelyek gyakran akadályozhatják az új technológiák széles körű elterjedését.

Ezen javaslatok figyelembevételével a megvalósítás során a pénzügyi intézetek, kereskedők és technológiai szolgáltatók egy egységes frontként működhetnek együtt a bankkártyák biometrikus azonosítással való kiváltásának előmozdításában. Az így kialakuló kooperáció nemcsak a fizetési rendszerek hatékonyságát és biztonságát erősíti meg, hanem a felhasználói elégedettséget is növeli, létrehozva egy olyan környezetet, amely ösztönzi az embereket a hagyományos bankkártyák helyett a modern, biometrikus alapú fizetési megoldások használatára.

5.3. További kutatási lehetőség

A biometrikus azonosítás területén további kutatási lehetőségek kínálkoznak a költségek és hozzáférhetőség kapcsán, különösen figyelembe véve az esetleges egyenlőtlenségeket a társadalom különböző rétegei között. Fontos felfedezni, hogy milyen tényezők járulnak hozzá a biometrikus azonosítási rendszerek elérhetőségének és költségeinek alakulásához, és hogyan lehet ezeket a kihívásokat kezelni a rendszerek széles körű elfogadásának és használatának érdekében.

Hogyan lehet a pénzügyintézetek, technológiai vállalatok és egyéb érintettek közötti együttműködéseket optimalizálni a biometrikus azonosítás sikeres bevezetése érdekében? Az együttműködési modellek és stratégiák tanulmányozása elősegítheti a fenntartható és hatékony implementációt.

Milyen hatással lehetnek a biometrikus fizetések az adatbiztonságra, és milyen kutatási irányok nyílnak meg ezen a területen? Fontos megérteni, hogyan lehet maximalizálni a biometrikus adatok védelmét, és miként lehet megelőzni az esetleges visszaéléseket vagy az adatlopás kockázatát. Az adatbiztonsági protokollok, az adatkezelési eljárások és az esetleges jogi szabályozások körében végzett kutatások segíthetnek kialakítani a biztonságos biometrikus fizetési rendszereket és elősegíthetik azok elfogadását a szélesebb társadalmi körökben.

Milyen mértékben fenntartható és skálázható a biometrikus azonosítás bevezetése a pénzügyi rendszerekben? A technológia hosszú távú hatásainak és fenntarthatóságának elemzése segíthet a hosszú távú siker érdekében szükséges intézkedések meghozatalában.

6. ÖSSZEFOGLALÁS

Az empirikus kutatás eredményeinek részletes elemzése rávilágított arra, hogy a Z generáció jelentős része pozitívan fogadja a biometrikus azonosítással történő fizetési módokra való átállást. A fiatalabb generációk pozitív fogadtatása pedig azt mutatja, hogy a biometrikus bankkártyák iránti érdeklődés és elfogadás a jövőben tovább növekedhet.

A kutatás eredményei továbbá azt sugallják, hogy a biometrikus azonosítás rutinszerű alkalmazása nagyobb részben kényelmes és hatékony azonosítást eredményez nem csupán a Z generáció számára, ami hozzájárul a vásárlási élmény pozitív irányú változásához. A kényelem és a hatékonyság az egyik fő döntési tényező a rendszer használata mellett.

A kutatás eredményei így alátámasztják azt az elképzelést, hogy a biometrikus azonosítással támogatott fizetési megoldások egyre inkább integrálódnak a mindennapi pénzügyi tevékenységekbe, így evvel is lassan fokozatosan növelve az idősebb generáció köreiből az elfogadottságot, valamint a jövőben további terjedésre számíthatunk ezen technológia terén.

Ugyanakkor a vizsgálat arra is rámutatott, hogy a biometrikus azonosítás nem feltétlenül jár számottevően rövidebb tranzakciós idővel a bankkártyákhoz képest. Az eredmények alapján tehát a hatékonyság szempontjából nem minden esetben hoz jelentős gyorsulást a biometrikus azonosítás alkalmazása. Annak hátterében, hogy mégis ekkora elfogadottságnak örvend a technológia az állhat, hogy a biometrikus azonosításnak más értékei is fontosak lehetnek a felhasználók számára. Például a kényelem, a biztonságérzet vagy a felhasználói élmény pozitív irányú változása.

A visszajelzéseken keresztül kiderül, hogy az ujjlenyomat-alapú biometrikus azonosítás nemcsak hatékony, hanem elfogadott és preferált is a felhasználók körében. Az észlelt biztonság, a gyorsaság és a felhasználóbarát felhasználói élmény együttesen hozzájárulnak ahhoz, hogy az ujjlenyomat-azonosítás egy kulcsfontosságú és népszerű megoldásnak bizonyuljon a biometrikus technológiák palettáján. Ez további kutatásokra és fejlesztésekre ösztönözhetik az ujjlenyomattal történő azonosítási rendszereket.

Az első javaslat tehát ebből kifolyólag az, hogy ezt a módszert implementálják elsősorban a pénzügyi intézetek a bankkártyák kiváltására.

Fontos továbbá, hogy folyamatosan történjen a bankok felől az ügyfeleinek számára a nyújtott edukáció, hogy megismerkedhessenek a technológiával és a használatával meggyőzve őket a rendszer kényelmességéről, biztonságáról és nem utolsósorban biztonságáról. Mindemellett kulcsfontosságú a velük való szoros kommunikáció kialakítása a projekt egész életciklusa alatt. Ez egyben járul hozzá a rendszer

felhasználóbarát kialakításához, és emellett nagyban növeli a módszer elfogadottsági rátáját.

A megvalósításnál elsősorban apró kis lépésekben érdemes bevezetni. Ezen lépés során a rendszer működése alaposan felmérhető, az esetleges hibák és hiányosságok kiküszöbölhetők, és a felhasználói tapasztalatok alapján további finomhangolások végezhetők. Érdemes lenne egyidőben néhány ujjenyomat azonosítóval felszerelt bankautomaták telepítésével. Ez további információval láthatná el a pénzügyintézeteket a rendszer fogadtatásáról, esetleges észrevételekről és hibákról.

Az ilyenféle új technológiai fejlesztések sikere szempontjából kardinális jelentőségű az együttműködés szorosabbá tétele a bankok, kereskedők és technológiai szolgáltatók között. Ez lehetőséget kínál a szabványok kialakítására, amelyek alapvető fontosságúak az új technológiai rendszerek széleskörű elfogadásához és integrációjához, mindemellett hozzájárulna a rendszerek kompatibilitásához, legfőképpen más pénzügyintézetek rendszerei közötti összeférhetőségéhez.

Az ilyen típusú innovatív projektek gyakran magas költségekkel járnak, és a vállalkozásoknak előnyös lehet, ha különböző finanszírozási források után kutatnak. Egyik potenciális lehetőség az állami támogatások és pályázatok.

A rendszerbiztonsági intézkedések kiemelt célja az illetéktelen hozzáférés, a csalások és a biztonsági hiányosságok megelőzése, ezzel erősítve a felhasználók bizalmát. Az adatvédelem terén kiemelten fontos a magas szintű garanciák biztosítása a biometrikus adatok kezelése során.

IRODALOMJEGYZÉK

- [1] HAZAI Lászlóné (2019): Módszerek, technikák a biometrikus arcfelismerésben,-azonosításban. Belügyi Szemle, 67(1), 118-126.
- [2] VARGA Domonkos – OLÁH András: Biometrikus azonosító rendszerek.
- [3] TAJTI Balázs (2012): A biometrikus ujjnyomat azonosítás alkalmazásának új lehetőségei. Hadmérnök, 8: 1.
- [4] NAGY Klára (2010): A biometrikus azonosítás új iránya.
- [5] KOVÁCS T. – MILÁK, I. – OTTI, C. (2012): A biztonság tudomány biometriai aspektusai. A biztonság rendészettudományi dimenziói: Változások és hatások, Budapest: Magyar Rendészettudományi Társaság, 485-496.
- [6] PALLAGI András (2020): Kontaktusmentes biometrikus azonosítási módszerek múltja, jelene és jövője. Rendészet-Tudomány-Aktualitások, 166-172.

Elektronikus hivatkozások

1. https://www.recoware.hu/biometria/biometriai_azonositas/arc.html (Utolsó letöltés: 2023. 11. 27.)

TARTALMI KIVONAT

A kutatás ismerteti a különböző biometrikus azonosítási módok működését, valamint betekintést nyújt, hogy hol találkozhatunk napjainkban is ezekkel a technológiákkal. Ezt követően hipotéziseket támaszt a különböző biometrikus azonosításokkal kapcsolatban kitérve azok elfogadottságára, kényelmére és hatékonyságára. Az állított feltevéseket aztán egy kvantitatív szemléletmódú primer kutatás segítségével vizsgálja, hogy elfogadhatóak-e, vagy pedig elvetendőek.

Végül különböző javaslatokat fogalmaz meg, amely során kitér arra, hogy mely biometrikus azonosítást lenne érdemes használni. Megfogalmaz továbbá az implementációt segítő ajánlásokat, amelyek az elősegíthetik a rendszerek elfogadottsági rátájának növekedését és a megvalósítás zökkenőmentesebbé tételét.

SUMMARY

The research describes the operation of different biometric identification methods, as well as provides insight into where these technologies can still be found today. After that, it raises hypotheses about different biometric identifications, focusing on their acceptance, convenience and efficiency. The stated assumptions are then examined with the help of primary research with a quantitative approach to see if they are acceptable or should be rejected.

Finally, it formulates different proposals, during which it discusses which biometric identification should be used. It also formulates recommendations to help implementation, which can help increase the acceptance rate of the systems and make the implementation smoother.