

Mellékletek

Biometrikus jellemzők		
Fizikai jellemzők	Viselkedésbeli jellemzők	Kombinált jellemzők
Ujjlenyomat	Járásmód	Hang/Beszéd
Tenyérlenyomat	Billentyűleütés	Aláírás
Kéz geometria	P300 agyhullámok mozgása	Kézírás
Arc geometria		
Fül alak		
Írisz mintázat		
Retina mintázat		
Vérerek mintázata		
DNS		

Tablázat 1 - A biometrikus jellemzők osztályozása

<i>Szerzők és publikáció éve</i>	<i>Minta</i>	<i>Vizsgált technológia</i>	<i>Használt elmélet(ek)</i>	<i>Fő eredmények</i>
Yang et al. (2015)	Kína 310 kitöltő	Mobilfizetés	Bizonytalansági-kockázat érték keretrendszer (Észlelt kockázat elmélet+ Kilátáselmélet+ Észlelt értékelmélet)	FR → UI: erős szignifikáns kapcsolat PR → UI: erős szignifikáns kapcsolat
Reepu & Arora (2022)	India 226 női kitöltő	Online banking	Észlelt kockázat elmélet	PR → UI: erős szignifikáns kapcsolat
Liébana-Cabanillas et al. (2024)	Spanyolország 2586 okostelefon felhasználó	Biometrikus mobilfizetés PayEye alkalmazás	UTAUT2 Észlelt kockázat elmélet	PE → UI: erős szignifikáns kapcsolat EE → UI: erős szignifikáns kapcsolat HM → UI: erős szignifikáns kapcsolat Észlelt kockázat → UI: erős szignifikáns kapcsolat
Zarco et al. (2024)	Spanyolország 1905 kitöltő 20 FinTech szakértő	Biometrikus bankkártya	UTAUT2 Általános észlelt kockázat elmélet Észlelt bizalom elmélet	Észlelt kockázat → UI: erős szignifikáns kapcsolat Észlelt bizalom → UI: erős szignifikáns kapcsolat SN → UI: erős szignifikáns kapcsolat

Tablázat 2 - Áttekintett kutatások összefoglalása

<i>Változók</i>		<i>Komponens</i>	<i>Forrás</i>
Várható teljesítmény (Performance Expectancy) – PE	PE1	A biometrikus fizetési megoldások használata hasznosnak bizonyulna a mindennapjaim során.	
	PE2	A biometrikus fizetési megoldások használata segítene a tranzakciók gyorsabb lebonyolításában.	Liébana-Cabanillas et al., 2024
	PE3	A biometrikus fizetési megoldások használata növelné a produktivitási szintem.	
Várható erőfeszítés (Effort Expectancy) – EE	EE1	Könnyen megtanulható lenne a biometrikus fizetés használata.	
	EE2	A biometrikus használata világos és érthető lenne.	
	EE3	A biometrikus fizetéshez szükséges készségeket könnyen elsajátítanám.	Liébana-Cabanillas et al., 2024
	EE4	Könnyűnek találnám a biometrikus fizetés használatát.	
Szubjektív normák (Subjective Norms) – SN	SN1	A számomra fontos személyek szerint, kellene biometrikus fizetési megoldásokat használnom.	
	SN2	A számomra fontos személyek egyet értenének azzal, ha biometrikus fizetési módszereket használnék.	Liébana-Cabanillas et al., 2024
	SN3	A számomra fontos személyek elvárják tőlem, hogy biometrikus fizetési módszereket használjak.	
	SN4	A legtöbb személy, akinek a véleményét értékelem, úgy gondolja, hogy kellene biometrikus fizetési megoldásokat használnom.	
Elősegítő feltételek (Facilitating Conditions) – FC	FC1	Rendelkeznék a biometrikus fizetéshez szükséges erőforrásokkal.	
	FC2	Rendelkeznék a biometrikus fizetéshez szükséges ismeretekkel.	
	FC3	Segítséget kaphatnék másoktól, ha nehézségeim lennének a biometrikus fizetés használatával.	Liébana-Cabanillas et al., 2024
Hedonikus motiváció (Hedonik motivation) – HM	HM1	A biometrikus fizetés használata izgalmas lenne.	
	HM2	A biometrikus fizetés használata nagyon szórakoztató lenne.	Liébana-Cabanillas et al., 2024
	HM3	Élvezném a biometrikus fizetés használatát.	
Megszokott viselkedés (Habit) – HAB	HAB1	A biometrikus fizetés használata szokássá válna számomra.	
	HAB2	A biometrikus fizetés használata természetessé válna számomra.	Liébana-Cabanillas et al., 2024
	HAB3	Úgy érzem, muszáj lenne használnom a biometrikus fizetést.	
Észlelt pénzügyi kockázat (Perceived Financial Risk) - PR	PR1	A bankszámlámra vonatkozó adatok kiszolgáltatottak lennének, abban az esetben, ha használnám a biometrikus fizetést.	
	PR2	Nagy esély van pénzbeli veszteségre, abban az esetben, ha használnám a biometrikus fizetést.	Yang et al., 2015
	PR2	Indokolatlan díjakat vonnának le, abban az esetben, ha használnám a biometrikus fizetést.	

Észlelet adatvédelmi kockázat (Perceived Privacy Risk) - PR	PR1	Nagy esély van arra, hogy a személyes adataim nem kívánt célokból is fellennének használva, abban az esetben, ha használnám a biometrikus fizetést.	Yang et al., 2015
	PR2	A személyes adataim nem megfelelően lennének megosztva és eladhatják őket, abban az esetben, ha használnám a biometrikus fizetést.	
	PR3	A személyes adataimhoz más, nem kívánt személyek is könnyen hozzáférhetnének, abban az esetben, ha használnám a biometrikus fizetést.	
Használati szándék (Use Intention) -UI	UI1	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, szándékomban állna használni vásárlásaim során.	Liébana-Cabanillas et al., 2024
	UI2	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, a következő néhány hónapban használnám vásárlásaim során.	
	UI3	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, szándékomban állna rendszeresen használni vásárlásaim során.	

Táblázat 3 - Kérdőív szerkezete

Pozitív magatartás	Gyorsaság
	Kényelem
	Biztonság
Negatív magatartás	Nehéz elfogadás
	Intruzív
Semleges magatartás	Tartózkodás

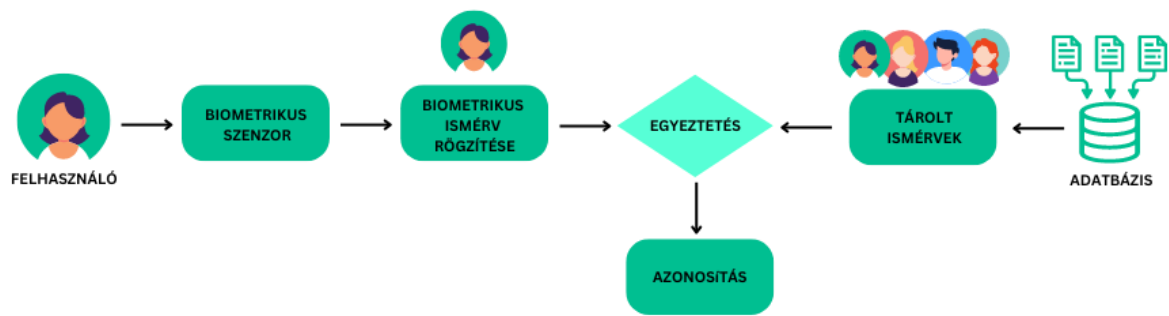
Táblázat 4 - A nyílt kérdések elemzésének összefoglalása

<i>Faktor</i>	<i>Komponens</i>	<i>Faktorsúlyok</i>	<i>Cronbach's alfa</i>	<i>Composite reliability</i>	<i>Average variance extracted (AVE)</i>
PE	PE1 PE2 PE3	0.945 0.945 0.921	0.931	0.931	0.878
EE	EE1 EE2 EE3 EE4	0.909 0.903 0.904 0.931	0.933	0.943	0.831
SN	SN1 SN2 SN3 SN4	0.876 0.761 0.813 0.902	0.859	0.868	0.705
FC	FC1 FC2 FC3	0.837 0.798 0.869	0.785	0.803	0.697
HM	HM1 HM2 HM3	0.938 0.936 0.962	0.940	0.943	0.894
HAB	HAB1 HAB2 HAB3	0.913 0.931 0.849	0.880	0.885	0.807
FR	FR1 FR2 FR3	0.892 0.922 0.838	0.860	0.863	0.783
PR	PR1 PR2 PR3	0.904 0.950 0.953	0.931	0.983	0.876
UI	UI1 UI2 UI3	0.963 0.953 0.956	0.954	0.954	0.916

Táblázat 5 - Faktorelemzés során vizsgált mutatók

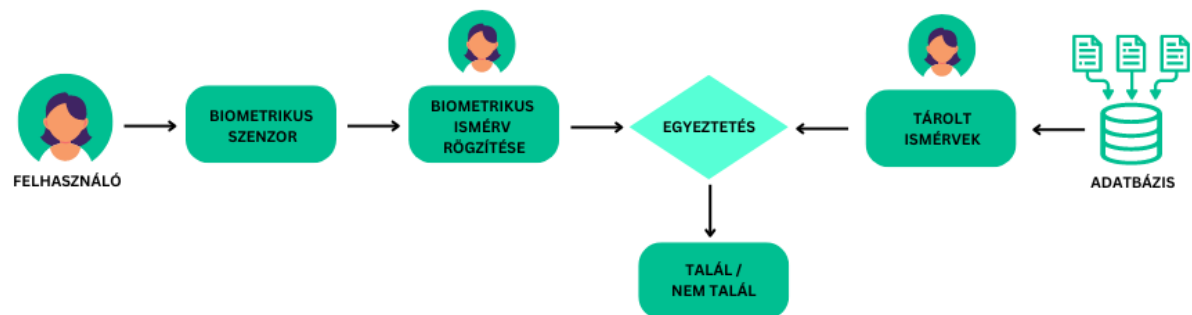
<i>Hipotézisek</i>	<i>Útegyüttható (path coefficient)</i>		<i>Szórás</i>	<i>T-statisztika</i>	<i>P-érték</i>	<i>Kapcsolat</i>
	<i>Eredeti minta</i>	<i>Mintaátlag</i>				
H1 PE→UI	0.262	0.263	0.086	3.064	0.002	Van
H2 EE → UI	0.100	0.099	0.082	1.233	0.218	Nincs
H3 SN→UI	0.120	0.117	0.066	1.814	0.070	Van
H4 FC→UI	-0.039	-0.034	0.054	0.711	0.477	Nincs
H5 HM→UI	0.059	0.065	0.123	0.483	0.629	Nincs
H6 HAB→UI	0.413	0.406	0.100	4.138	0.000	Van
H7 FR→UI	-0.113	-0.115	0.070	1.618	0.106	Nincs
H8 PR→UI	-0.010	-0.009	0.061	0.166	0.868	Nincs

Táblázat 6 - A hipotézisek tesztelése



Ábra 1 – Identifikációs folyamat

Forrás: Manisha & Kumar, 2020, 1. o. alapján, saját szerkesztés



Ábra 2 – Verifikációs folyamat

Forrás: Manisha & Kumar, 2020, 1. o. alapján, saját szerkesztés

1. **Melléklet** – Biometrikus rendszerek működésének leírása

Ujjlenyomat alapú azonosítás: Az egyik legnépszerűbb és legrégebb biometrikus azonosítási forma az ujjlenyomat beolvasása (Kodituwakku, 2015). Ezen azonosítási módszert a szakirodalomban daktiloszkópiának is nevezik (Babisch, 2012). Az ujjlenyomatot képző minták egyediak, az egyetértő ikrek esetében is, így meghatározható egy egyén személyazonossága (Kumar & Ryu, 2009). Az ujjlenyomatot beolvasó rendszerek az ujjbegyeken levő barázdákat osztályozzák, olyan mikroszkópikus részletek szerint, mint például a barázdák végpontjai és elágazásai (Kumar & Ryu, 2009), továbbá vizsgálják az íveket és hurkokat is (Sreekumar, 2010), valamint egyes technológiák a barázdák közötti pórusokat is felméri (Kumar & Ryu, 2009).

Az ujjlenyomatok beolvasása már több, mint száz éve jelen van az igazságszolgáltatásban, az egyik legfeljettebb és legpontosabb azonosítási módszer, valamint ezen rendszerek a legolcsóbbak közé sorolhatóak. Emellett az egyik legegyszerűbben használható biometrikus technológia (Clodfelter, 2010), valamint szinte azonnali hozzáférést nyújt egy adott rendszerhez (Kumar & Ryu, 2009). Napjainkban világszerte a legsűrűbben használt biometrikus azonosítási módszer (Liébana-Cabanillas et al., 2024).

Tenyérlenyomat és kéz geometria alapú azonosítás: A tenyérlenyomat a kezek tenyér részéről beolvasott képet jelképezi. Ezen lenyomat is könnyen megkülönböztethető és beolvasható különböző eszközökkel, hasonlóan az ujjlenyomat beolvasó technológiákhoz. A tenyér mintázata három fő elemből tevődik össze: elsődleges vonalak, másodlagos vonalak, valamint barázdák. Két tenyér mintázatának összehasonlítása során, olyan információk is figyelembe vannak véve, mint például a bemélyedések és a bőr textúrája (Babisch, 2012).

A kézgeometria esetében, a teljes kéz mérete és formája beolvasásra kerül (Clodfelter, 2010). Az azonosítás érdekében a rendszer olyan jellemzőket mérhet, mint például a kéz vagy az ujjak szélessége, hosszúsága, illetve a kéz felületének nagysága (Kumar & Ryu, 2009). A kéz beolvasására használt szkennelő rendszerek nagyon pontosak, azonban viszonylag drágák (Clodfelter, 2010).

Arcfelismerésen alapuló azonosítás: Egy személy arcának megtekintése a legegyszerűbb módja egy adott személy felismeréséhez. Az arcfelismerést, hagyományos, nem biometrikus technológiát alkalmazva, számos területen használatra kerül, például a jogosítvány, a személyazonosító igazolvány, illetve egyes bankkártyák esetében. Ezen helyzetben csupán egy kép készül a felhasználóról (Sreekumar, 2010).

Az arcfelismerő technológiák egy egyén különböző arcvonásait elemzi (Clodfelter, 2010). Az ember arcát illetően, számos megkülönböztethető pont létezik, 80 csomópontot azonosít be az arc IT, ezen pontok pedig különböző képpen mérhetőek, például a szemek közötti távolsági pontok, a szeme görbületi mélysége, az orr szélessége, az arccsontok alakja, valamint az állkapocsvonal hosszúsága. Ezen csomópontok mérését követően, a rendszer létrehoz egy numerikus kódot, amely az arclenyomatot képezi az adatbázisban. A használt rendszerektől függően történhet 2D vagy 3D mérés (Babisch, 2012).

Az arcfelismerés világszerte a második leghasználtabb biometrikus technológia, az ujjlenyomatot követően (Liébana-Cabanillas et al., 2024).

Írisz felismerésen alapuló azonosítás: Az írisz, a szemben található színes rész, amely körülveszi a pupillát. Jelen biometrikus technológia arra alapozódik, hogy minden egyén szemében található írisz mintázat és szín egyedi, így ezen összetett szerkezet hozzájárul a jellemzők összehasonlításához (Kodituwakku, 2015). Az írisz jellemzői körülbelül 10-60 cm távolságtól is beolvashatóak, a mérés során az egyén, nyugodt állapotban, egy kamerába kell nézzen, ameddig befejeződik az elemzés (Clodfelter, 2010).

A szakértők véleménye szerint az írisz mintázata egyedibb, mint a hópelyhek mintázata, így az egyik leígéretesebb eszközök közé sorolható. Az írisz beolvasása során, egy digitális kamera segítségével egy kép készül a szemről, illetve a rendszer regisztrálja az egyén íriszének mintázatát. Abban az esetben amikor egy személy beszkeneli a szemét, hogy például beléphessen egy adott intézménybe, akkor a kamera összehasonlítja az adatbázisban levő képeket, a beolvasott írisz mintával a döntéshozatal érdekében. A folyamat gyors, pár másodpercet igényel (Clodfelter, 2010).

Egyes fogyasztók véleménye szerint ezen megoldás, sokkal inkább tolatodóbbnak számít, az ujjlenyomat leolvasásához képest, míg a kínai felhasználók szerint sokkal higiénikusabb megoldást feltételez (Clodfelter, 2010).

2. **Melléklet** – Biometrikus fizetési megoldások előnyeinek és hátrányainak bemutatása

A biometrikus azonosítás és fizetés számos előnnyel rendelkezik (Mróz-Gorgoń et al., 2022; Kim et al., 2019). A legnagyobb előnyt a kimagasló biztonság és védelem jelenti a felhasználók számára (Clodfelter, 2010). A bankok minimalizálhatják a nem jogosult, hamis hozzáférést, autentifikációt (Liébana-Cabanillas et al., 2024), valamint abban az esetben, ha az ügyfél elveszíti vagy ellopják bankkártyáját, nem kell azzal a kockázattal szembesülnie, hogy egy nem kívánt személy felhasználja azt (Clodfelter, 2010). Ezen fizetési módszer, egy gyorsabb megoldást nyújt a vásárlóknak, körülbelül 70%-kal felgyorsíthatja a pénztárnál történő fizetést (Kumar & Ryu, 2009).

Egy további előny a kényelem, ugyanis a fogyasztónak nem szükséges magával vinnie pénztárcáját, a különböző bankkártyáit vagy mobiltelefonját (Kim et al., 2019), valamint nem szükséges a jelszavak észbetartása (Zarco et al., 2024). A költségmegtakarítás is egy előnyt jelenthet, ugyanis a fokozott biztonság miatt, a csalási arány is alacsonyabb lehet, ezáltal a visszaigénylések száma is csökkehet. A feldolgozási és tranzakciós díjak is egyes esetekben alacsonyabbak, a hitelkártyákkal szemben (nttdatapay.com, 2024). Emellett a környezetvédelem is az előnyök közé sorolható, ugyanis a legtöbb biometrikus fizetési megoldások esetében, nem szükséges a bankkártyák gyártása, így nem kerül felhasználásra műanyag, amely nagymértékben csökkentheti a környezetszennyezést (Kim et al., 2019).

Az előbbieken említett előnyök mellett, ezen technológia különböző hátrányokat is feltételez (Kim et al., 2019). Annak ellenére, hogy a biometrikus azonosítás magas biztonsági szintet és védelmet nyújt, ezen technológia mégsem jelent egy tökéletes megoldást (Kodituwakku, 2015). Bár ritka az előfordálása, de egyes esetekben megtörténhet, hogy hamis elfogadás történik a rendszer részéről. Összkeverednek az egyének biometrikus adatai ikrek vagy hasonló személyek esetében, ha az adatbázisban nem megfelelően voltak rögzítve az adatok vagy abban az esetben, ha a biometrikus szenzor nem megfelelően volt kalibrálva. Ezen hiba fordítottja is megtörténhet, amikor a beolvasó elutasít egy legitim személyt. Téves elutasítás megtörténhet abban az esetben, ha például a kép elmosódik vagy az egyén egyes jellemzői megváltoznak, például arcfelismerés esetében, a személy megjelenése változik súlygyarapodás vagy fogyás során. Egyes kultúrákhoz tartozó személyek esetében a hamis elfogadás magasabb,

fontos, hogy ezen rendszerek inkluzívak legyenek, ne merüljön fel kultúrális vagy demográfiai diszkrimináció (Othman, 2024).

Egyes személyek számára, a biometrikus technológián alapuló rendszerek használata kényelmetlen lehet, kultúrális okok, valamint vallási okok miatt (Clodfelter, 2010).

Egy további hátrány, az adatvédelmi aggályokat feltételezi, a felhasználók kockázatot érzékelnek az adataikkal szemben, tartanak attól, hogy a rögzített és tárolt adatokat feltörhetik és nem kívánt célokból, más személyek is felhasználhatják (Kim et al., 2019). Bár a biometrikus technológia általánosan véve biztonságosabb és nehezebben feltörhető, mint a jelszavak és a PIN kódok, vannak helyzetek amikor, például arcfelismerő rendszerek esetében, fényképek segítségével megtevesztik a rendszert és hozzáférnek az adott személy pénzügyeihez és adataihoz (Liébana-Cabanillas et al., 2024). Egy másik hátrány abból adódik, hogy ellentétben a hagyományos fizetési rendszerekkel, ahol a jelszó vagy a PIN kód módosítható, a biometrikus adatok nem módosíthatóak (Zarco et al., 2024).

Emellett hátrányt jelenthet az infrastruktúra kialakítása, ahhoz hogy ezen fizetési megoldás használható legyen, szükséges speciális szenzorok és rendszerek beszerelése a kereskedelmi egységekbe (Kim et al., 2019).