Magyar Rendészet 2026/1. 205–223.
DOI: 10.32577/MR.2026.1.14

KRIMINALISZTIKA

A biometrikus azonosítás és az adatvédelem

Biometric Identification and Data Protection

BOJTÁR J. Tamás,[1] TÓTH Attila[2]

Bevezetés: A digitális korszakban a pénzügyi szektor egyik legnagyobb kihívása az ügyfél-azonosítás biztonságos és adatvédelmi szempontból is megfelelő megvalósítása. A biometrikus azonosítás – ujjnyomat, írisz, arcfelismerés – egyre elterjedtebb a bankbiztonságban, azonban az ezekhez kapcsolódó érzékeny személyes adatok tárolása és kezelése komoly adatvédelmi kockázatot hordoz. A biometrikus jellemzők megváltoztathatatlanok, így illetéktelen hozzáférés esetén a károsodás visszafordíthatatlan.

Célkitűzések: A tanulmány bemutatja, miként járulhat hozzá a homomorf titkosítás és a decentralizált adattárolás a biometrikus adatok védelméhez, és hogyan növelhető a rendszerek biztonsága anélkül, hogy az azonosítás hatékonysága csökkenne. A kutatás célja a bankbiztonsági gyakorlat adatvédelmi kihívásainak feltárása és a legújabb technológiai irányok elemzése.

Módszertan: A vizsgálat szakirodalmi elemzést, a jogszabályi és szabványi környezet áttekintését foglalta magában, valamint primer adatgyűjtést: kérdőíves felmérést és félig strukturált interjúkat bankbiztonsági, információbiztonsági, adatvédelmi szakemberekkel, továbbá a centralizált és decentralizált tárolási modellek összehasonlítását.

Eredmények: A felmérés eredményei szerint a válaszadók 62,5%-a hallott már a homomorf titkosításról, közülük 96,7% alkalmazhatónak tartotta a biometrikus adatok védelemére. A decentralizált tárolást 79,2% ismerte, 82,9% szerint a biometrikus adatok védelmét erősíti ez a fajta adattárolás.

Konklúzió: A szakértői interjúk megerősítették, hogy ezek a technológiák jelentősen csökkentik az adatlopás és -szivárgás kockázatát, miközben támogatják a GDPR *privacy by design* elvét. Az eredmények alátámasztják a kutatott technológiák kockázatcsökkentő hatékonyságát, hangsúlyozva a *privacy by*

[1] Hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, e-mail: thomas.doubting1@gmail.com
[2] PhD, adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, e-mail: toth.attila@uni-nke.hu

design elv érvényesítését és a szabályozási finomhangolás szükségességét a gyakorlati integrációhoz.

Kulcsszavak: biometrikus azonosítás, adatvédelem, bankbiztonság, homomorf titkosítás, decentralizált adattárolás

Introduction: In the digital era, one of the greatest challenges faced by the financial sector is implementing customer identification in a manner that is secure and compliant with data protection requirements. Biometric identification – including fingerprints, iris patterns and facial recognition – is becoming increasingly prevalent in banking security. However, the storage and processing of such sensitive personal data pose significant privacy risks, as biometric traits are immutable, and any unauthorised access may result in irreversible harm.

Objectives: This study explores how homomorphic encryption and decentralised data storage can enhance the protection of biometric data and strengthen system security without compromising the efficiency of authentication. The primary objective is to identify the main data protection challenges within banking security practice and to analyse emerging technological trends addressing these risks.

Methodology: The research combines a comprehensive literature review, an analysis of the relevant legislative and standardisation framework, and primary data collection. Empirical data were obtained through a questionnaire survey and semi-structured interviews with professionals in banking security, information security and data protection, coupled with a comparative assessment of centralised and decentralised data storage models.

Results: The empirical findings reveal that 62.5% of respondents were familiar with homomorphic encryption, and 96.7% of them regarded it as a viable method for protecting biometric data. Additionally, 79.2% were aware of decentralised storage, with 82.9% recognising it as a solution that enhances the protection of biometric information.

Conclusion: Expert interviews confirmed that these technologies significantly reduce the risks of data theft and leakage, while supporting the application of the GDPR's privacy by design principle. The findings validate the risk-reduction effectiveness of the examined technologies and underscore the importance of enforcing privacy by design and fine-tuning regulatory frameworks to facilitate their practical integration.

Keywords: biometric identification, data protection, bank security, homomorphic encryption, decentralised storage

A banki azonosítás jövője: biometrikus kockázatok és korszerű védelmi architektúrák

A pénzügyi szektor digitalizációja radikálisan átalakította a banki azonosítási gyakorlatot. A biometrikus azonosítás – ujjlenyomat, ujjnyomat (Ujhegyi 2023), arcfelismerés, írisz – kényelmes és gyors, de adatvédelmi szempontból különösen érzékeny, hiszen a biometrikus jellemzők megváltoztathatatlanok, így ha ezek az adatok illetéktelen kezekbe kerülnek, a károsodás visszafordíthatatlan.

A cél annak feltárása, hogy milyen módon lehet védeni ezeknek az adatoknak a biztonságát korszerű technológiákkal – titkosítással és decentralizált adattárolással – anélkül, hogy az azonosítás hatékonysága csökkenne.

A biometrikus azonosítás és az adatvédelem kérdésköre nem kizárólag technológiai vagy jogi probléma, hanem a rendészettudomány, a magánbiztonság és az információbiztonság határterületén elhelyezkedő, interdiszciplináris kutatási irány. A hazai tudományos diskurzusban az elmúlt évtizedben megfigyelhető a biztonságtudományi és adatvédelmi témák intézményesülése, valamint a magánbiztonság és az információvédelem iránti növekvő tudományos érdeklődés. E folyamatot jól szemlélteti a Nemzeti Közszolgálati Egyetem Magánbiztonsági és Önkormányzati Rendészeti Tanszék publikációs tevékenységének tudománymetriai elemzése, amely rámutat arra, hogy a biztonságtechnológia, az adatvédelem és a kiberbiztonság kérdései egyre hangsúlyosabb szerepet töltenek be a hazai rendészettudományi kutatásokban, és szoros kapcsolatban állnak a gyakorlati biztonsági kihívásokkal. Mindez alátámasztja, hogy a biometrikus azonosítás adatvédelmi vizsgálata nem elszigetelt kutatási terület, hanem egy fejlődő, intézményesen is megerősödött tudományos környezetbe illeszkedik (Csaba–Tóth 2024).

A biometrikus adatok a GDPR, az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete szerint „különleges adatnak" számítanak, ami miatt kezelésük csak szigorú jogalappal – például kifejezett hozzájárulással vagy más törvényes indokkal – és megfelelő adatvédelmi garanciákkal lehetséges.

Az elemzett szakirodalom rámutat, hogy a biometrikus adatok kezelése különös figyelmet igényel, és az adatkezelés során biztosítani kell az adatminimalizálást, a pszeudonimizálást[3] vagy anonimizálást,[4] illetve az erős technikai védelem alkalmazását. A biometrikus információk védelmére létezik nemzetközi szabvány is: ISO/IEC 24745, amely előírja az adatvédelem követelményeit, például a biometrikus sablonok védelmét.

Az adatvédelmi és kiberbiztonsági szabályozási környezetben Magyarországon emellett rámutatnak az egyre fontosabbá váló kiberbiztonságra: az új, 2024. évi LXIX. törvénynek Magyarország kiberbiztonságáról – a 2022-ben elfogadott, az Európai Parlament

[3] Pszeudonimizálás: álnevesítés, a személyes adatok olyan módon történő kezelése, amely során azok további információk nélkül már nem köthetők közvetlenül egy természetes személyhez, de megfelelő kulcsok birtokában visszaállíthatók (GDPR 4. cikk 5. pont). Ez adatvédelmi technikaként csökkenti a reidentifikáció kockázatát, miközben lehetővé teszi az adatok elemzését.

[4] Anonimizálás: a személyes adatok olyan visszafordíthatatlan átalakítása, amelynek eredményeként további információk nélkül többé már nem azonosítható a természetes személy, így az adatok kikerülnek a GDPR hatálya alól (GDPR preambulum 26.). Ez a legmagasabb szintű adatvédelmi technika, amely lehetővé teszi az adatok anonim elemzését.

és a Tanács (EU) 2022/2555 számú irányelve (NIS 2) hazai átültetése – célja a kritikus informatikai rendszerek és szolgáltatások biztonságának megerősítése. Ezzel összhangban pénzügyi, különösen banki környezetben már hosszabb ideje léteznek olyan jogszabályok és felügyeleti elvárások, amelyek kifejezetten az informatikai és kiberbiztonsági kockázatok kezelésére irányulnak: a 42/2015. (III. 12.) Korm. rendelet, a 29/2024. (VI. 24.) MNB rendelet, valamint a Magyar Nemzeti Bank 1/2025. (I. 13.) számú ajánlása, illetve annak jogelődei, amelyek már évek óta konkrét, kötelezően vagy elvárásként alkalmazandó követelményeket határoznak meg.

Ez összhangba hozza a biometrikus adatkezelés és -tárolás kérdését a szervezeti kiberbiztonsági követelményekkel, különösen pénzügyi intézmények esetében, ahol magas fokú adatvédelem és rendszerintegritás szükséges.

A kutatás középpontja, hogy a banki környezetben alkalmazott biometrikus rendszerek milyen adatvédelmi kockázatokkal szembesülnek, és hogyan kezelhetők ezek korszerű titkosítási eljárásokkal. A vizsgálat során szakirodalmi elemzés készült a biometrikus azonosítás és adatvédelem területéről, interjúk készültek bankbiztonsági és adatvédelmi szakemberekkel, valamint megtörtént a centralizált és decentralizált adattárolási modellek összehasonlítása. A kutatás hipotézise szerint a homomorf titkosítás és a decentralizált adattárolás együttesen képes növelni a biometrikus adatok védelmét, miközben fenntartja a gyors és hatékony azonosítást.

A téma kutatása során az iparági szakirodalmat és az elsődleges forrásokat dolgoztuk fel leginkább, például szakcikkek, tudományos publikációk, kutatási jelentések, bankbiztonsági ajánlások és irányelvek elemzésével az alábbi módszerek szerint:

- a biometrikus személyazonosítás hazai jogszabályi környezetének vizsgálata;
- a személyazonosításra vonatkozó speciális szabályok vizsgálata;
- az adatok védelmére vonatkozó szabályozók vizsgálata;
- a kutatás témakörét érintő bank- és információbiztonság, magánbiztonság, valamint az adatvédelem munkatársaival történő konzultáció;
- a biometrikus azonosítási technológiák és adatvédelmi irányelvek elemzése és összehasonlítása a bankbiztonság területén;
- a biometrikus azonosítás és adatvédelem által nyújtott előnyök és kockázatok felmérése és értékelése.

A publikációban foglaltak további kutatási alapként szolgálhatnak az általános banki azonosítás során használt biometrikus adatok kezelésében, valamint hozzájárulhatnak a bankbiztonsági rendszerek hatékonyságának növeléséhez és az általános államigazgatási reform folyamatába illeszkedő korszerűsítéshez.

A biometrikus azonosítás szerepe és működése a bankbiztonságban

A biometrikus azonosítás szerepe az elmúlt két évtizedben alapjaiban alakította át a biztonsági rendszerek működését, különösen a kritikus infrastruktúrák, szervezetek körébe tartozó pénzügyi intézmények esetében. A biometrikus technológiák lényege, hogy

az azonosítást olyan egyedi biológiai vagy viselkedési jellemzőkre építik, amelyek stabilak, tartósak és másolhatatlanok. Ezek közé tartoznak többek között az ujjnyomatok, az arcgeometria, az írisz mintázata, illetve a viselkedésalapú jellemzők, mint a kézírás vagy a beszédhang. A biometrikus azonosítás pontos definíciója szerint az egyén egyedi biometrikus adatait összevetik egy adatbázisban tárolt sablonnal, amely matematikai jellemzők halmaza, nem pedig a nyers kép vagy lenyomat (Grother–Salamon–Chandramouli 2013).

A biometrikus azonosítás technológiai előnye abban áll, hogy a személyazonosság megerősítéséhez nincs szükség olyan tudásalapú elemekre, mint a jelszó vagy PIN-kód, amelyek elveszíthetők, ellophatók vagy megfejthetők. A biometrikus jellemzők a személyhez kötöttek, nem ruházhatók át, és – ideális esetben – nem hamisíthatók. A modern biometrikus rendszerek fejlődése olyan technológiai személyiségeknek köszönhető, mint John Daugman, aki az íriszfelismerés algoritmusait (*Biographical sketch, John Daugman* [é. n.]) már 1994-ben ipari szintre emelte, illetve Mitchell Trauring, aki 1963-ban publikálta az első tudományos ujjlenyomat-illesztő algoritmust (Trauring 1963). A fejlődés következő szakaszát az olyan kutatók foglalják össze, mint például Anil K. Jain és társai, akik a biometria teljes modern ökoszisztémáját áttekintik (Jain–Nandakumar–Ross 2016).

A bankbiztonsági alkalmazásokban az ujjnyomat-azonosítás továbbra is kiemelt szerepet játszik, a stabilitása és bizonyító ereje miatt (Ujhegyi 2023). Emellett az íriszfelismerés és az arcfelismerés egyre fontosabb szerephez jut a belépés-ellenőrzési rendszerekben, különösen olyan helyzetekben, amikor a felhasználónak gyors, érintésmentes azonosításra van szüksége. Az arcfelismerés azonban egyszerre hordoz biztonsági előnyöket és társadalmi kockázatokat, amire Ujhegyi és szerzőtársa hívja fel a figyelmet, különös tekintettel a kínai megfigyelési gyakorlatokra (Ujhegyi–Kun 2020).

A biometrikus rendszerek működése szigorúan függ a háttér-technológiáktól: a mintavételtől a sablonképzésen át az összevetésig. A döntéshozatali folyamat pontosságát az algoritmusok minősége, a zajkezelés, a fényviszonyok, a testrészek állapota és a szenzorok érzékenysége befolyásolja. A bankok számára kulcsfontosságú, hogy minimalizálják a hamis elfogadás (FAR) és hamis elutasítás (FRR) arányát. A hamis elfogadás kiküszöbölésére való törekvés fontossága a biztonsági szakemberek számára talán nyilvánvalóbb, azonban a hamis elutasítás is komoly problémát okozhat, mivel jogosult ügyfelek nem férnek hozzá szolgáltatásokhoz, ami bizalomvesztést, ügyfélszolgálati többletköltséget és versenyhátrányt eredményez. Ráadásul a felhasználói frusztráció akár arra is ösztönözheti a felhasználót, hogy megkerülje vagy mellőzze a védelmi megoldást, amennyiben az adott alkalmazásban erre lehetőség van (Tiszolczi 2023), ez pedig olyan új rendszerek felé tereli a fejlesztést, mint a multimodális biometria, ahol több biometrikus jellemző együttesen határozza meg a személyazonosságot.

A biometrikus azonosítás a pénzügyi szektorban már nem kiegészítő technológia, hanem az alapbiztonság része. A fejlődést azonban jelentősen befolyásolja, hogy e személyes adatok kezelése milyen adatvédelmi garanciákkal párosul.

A biometrikus adatok adatvédelmi szabályozása és kérdései

A biometrikus adatok kezelése a GDPR egyik legérzékenyebb és legszigorúbban szabályozott területe. A rendelet kifejezetten különleges adatként kezeli a biometrikus információkat, mivel ezek olyan testi vagy viselkedési jellemzők, amelyekkel az érintett egyértelműen azonosítható. A biometrikus adat definícióját a GDPR egyértelműen rögzíti: „egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat."

A biometrikus azonosítók sajátossága, hogy nem megváltoztathatók, így kiszivárgás esetén nem lehet „új" ujjlenyomatot, arcképet vagy íriszmintázatot létrehozni. Éppen ezért hangsúlyozza Szabó Máté Dániel is, hogy a biometrikus azonosítás és az adatvédelem viszonya olyan egyensúlyi helyzetet igényel, ahol a technológiai előnyök nem veszélyeztetik az érintett magánszférát (Szabó 2004). A bankbiztonsági környezetben ez különösen fontos, hiszen a biometrikus adatok a pénzügyi infrastruktúrák egyik elsődleges védelmi vonalává váltak.

A GDPR nemcsak a fogalmakat definiálja (adatkezelő, adatfeldolgozó, adatvédelmi incidens, álnevesítés), hanem konkrét elveket is meghatároz: célhoz kötöttség, adattakarékosság, átláthatóság, korlátozott tárolhatóság. A biometrikus rendszerekben azonban ezek az elvek gyakran ütköznek a technológia működési logikájával. Az ujjlenyomat- vagy arcfelismerő rendszerek ugyanis tipikusan folyamatos összevetést és hosszú távú tárolást igényelnek, ez pedig újra és újra felveti a szükségesség és arányosság kérdését.

A gyakorlatban a legkritikusabb pont a biometrikus sablonok védelme (Grother–Salamon–Chandramouli 2013). A sablon elvileg nem állítható vissza nyers képpé, azonban nem megfelelő implementáció esetén a visszafejtés technikailag nem lehetetlen. Éppen ezért a modern adatvédelmi gyakorlat megköveteli, hogy a biometrikus sablonokat titkosított, elkülönített és visszavezethetetlen formában tárolják. A bankbiztonság sajátossága, hogy a biometrikus adatok kezelése kettős célhoz kötött: fizikai beléptetés és informatikai hozzáférés. Ebben az esetben a GDPR szerinti érdekmérlegelési teszt, valamint a kockázatalapú megközelítés válik hangsúlyossá (Lippai–Mezei 2024). A biometrikus adatok felhasználása ennél szélesebb körű is lehet, amelyekben további célok jelennek meg, így például az ügyfél-azonosítás – akár távoli csatornákon, például videóbanki alkalmazásokban –, valamint a csalásmegelőzés és a visszaélések detektálása, amelyek mind önálló adatkezelési célt és külön adatvédelmi értékelést tehetnek szükségessé.

Elmondható, hogy a biometrikus azonosítás nem lehet önmagában biztonsági garancia. A biometrikus adatok védelmének hiányossága ráadásul közvetlen fizikai következményekkel járhat a kritikus infrastruktúra működőképességére – például beléptetési zavarok, jogosulatlan behatolások formájában.

A valódi védelemhez olyan technológiák szükségesek, amelyek biztosítják, hogy a biometrikus sablonok sem nyugalmi helyzetben, sem használat közben ne legyenek visszafejthetők. Ezt a problémát oldja meg a homomorf titkosítás, amely lehetővé teszi az adatok titkosított formában történő feldolgozását.

Homomorf titkosítás és decentralizált tárolás a biometrikus adatok védelmében

A biometrikus adatok hosszú távú védelmének egyik legmodernebb és legígéretesebb megoldása a homomorf titkosítás (*fully homomorphic encryption,* FHE) (Gentry 2009). Ez a titkosítási forma lehetővé teszi, hogy a rendszer a biometrikus sablonokon úgy végezzen számításokat – például ujjlenyomat-összevetést –, hogy azok végig titkosított állapotban maradnak. Ez az áttörés gyökeresen megszünteti a klasszikus tárolási és működési kockázatokat: még akkor sem fejthető vissza a sablon, ha az adatbázis egy az egyben illetéktelen kézbe kerül.

Az FHE lényege, hogy a biometrikus összevetéshez szükséges matematikai műveletek – távolságszámítás, hasonlóságiindex-képzés – végrehajthatók a titkosított adatokon. Így a rendszer soha, egyetlen pillanatra sem fér hozzá a felhasználó tényleges biometrikus jellemzőihez. Ez technológiai szempontból a legmagasabb szintű adatvédelmi garancia, amely rendszerfüggetlenül ellenállóvá teszi az adatlopással, kompromittálással és rendszerszintű támadásokkal szemben.

A bankbiztonsági infrastruktúrák számára a másik kulcsfontosságú terület a decentralizált vagy megosztott tárolás. Ezek közös előnye, hogy nincs egyetlen támadható adatpont, így egyetlen biztonsági incidens sem eredményez teljes sablonszivárgást.

A homomorf titkosítás és a decentralizált tárolás egymást erősíti: az FHE biztosítja a működési titkosítást, a decentralizáció a strukturális ellenálló képességet. Modern megközelítésben a biometrikus sablonok már nem egyetlen központi adatbázisban léteznek, hanem több független komponensből állnak össze, amelyeket a rendszer csak a hitelesítési folyamat alatt – és ott is titkosítva – használ.

A viselkedésalapú biometria – például a gépelési ritmus (Ujhegyi–Kun 2020) vagy a járásminta (Chripko 2025) – különösen profitál az FHE-alapú feldolgozásból. Ezek az adatok is folyamatos gyűjtést és dinamikus összevetést igényelnek, így a folyamatos titkosított feldolgozás jelentős adatvédelmi előnyt biztosít. A decentralizált megoldások további előnye, hogy a felhasználók számára biztosítható a saját biometrikus adatok feletti kontroll: például a személy birtokolhatja az egyik kulcsrészletet, amely nélkül a rendszer nem képes hitelesítést végrehajtani. Ez a modell összhangban áll a GDPR *privacy by design* (az Európai Parlament és a Tanács 2016/679 rendelete, 25. cikk) megközelítésével.

A homomorf titkosítás és a decentralizált tárolás nemcsak technikai, hanem filozófiai fordulatot is jelent a biometrikus rendszerekben: a biometrikus adat többé nem egy titkosítva őrzött titok, hanem információ, amelyhez senki sem fér hozzá – még a rendszer sem. Ez a valódi adatvédelmi garancia.

Homomorf titkosításon alapuló alkalmazások

Microsoft SEAL

A Microsoft SEAL (Simple Encrypted Arithmetic Library) a homomorf titkosítás egyik legszélesebb körben használt, nyílt forráskódú könyvtára, amelyet a Microsoft Research

fejleszt és tart fenn. A könyvtár a BFV- és a CKKS-sémák implementációját biztosítja, lehetővé téve egész és lebegőpontos aritmetikai műveletek elvégzését titkosított adatokon úgy, hogy a visszafejtésre a számítási folyamat egyetlen pontján sincs szükség.

A SEAL implementációja modern rácsalapú *(lattice-based)* kriptográfiai konstrukciókra épül, amelyek a jelenlegi kutatási eredmények szerint kvantumszámítógépek ellen is védelmet nyújtanak. A könyvtár 2024-es kiadásai több optimalizációt tartalmaznak a memóriahasználat, a kulcskezelés és a zajnövekedés kontrollálása terén, ami különösen fontossá válik olyan alkalmazásoknál, ahol nagy mennyiségű, bonyolult szerkezetű adatot dolgoznak fel titkosított formában – ilyenek a biometrikus sablonok is.

A homomorf titkosítás paraméterezésére vonatkozó ajánlásokat a Homomorphic Encryption Standardization Working Group tartja karban. A 2024-es ajánlás külön kiemeli a SEAL által alkalmazott gyakorlati paraméterkészletek stabilitását és ipari alkalmazhatóságát (Albrecht et al. 2018).

A pénzügyi és biometrikus azonosítási környezetben a SEAL legfontosabb előnye, hogy lehetőséget biztosít a teljes hitelesítési folyamat titkosított adatállapot melletti végrehajtására. Ez azt jelenti, hogy a biometrikus sablonok – például ujjlenyomatból vagy arcképből származó jellemzők – összevetése során sem a rendszer, sem annak üzemeltetője, sem harmadik fél nem fér hozzá a tényleges mintákhoz. A folyamat így megfelel a *privacy by design* elvének, és jelentősen csökkenti a sablonszivárgásból eredő hosszú távú kockázatot.

Google Private Join and Compute

A Google Private Join and Compute (PJC) lehetővé teszi két szervezet számára, hogy úgy hasonlítsanak össze adatokat, hogy közben egyik fél sem látja a másik nyers adatait. A rendszer lényege, hogy a felek csak azonosító alapján keresik meg a közös rekordokat, majd kizárólag ezekről számolnak összevont eredményeket – például darabszámot vagy átlagot – úgy, hogy az egyéni adatok rejtve maradnak.

A PJC működése két technikára épül:

- az egyik a privát halmazmetszet (*private set intersection,* PSI), amely meghatározza, hogy mely rekordok közösek;
- a másik a titkosított számítás, amely biztosítja, hogy az adatok a feldolgozás teljes folyamata alatt titkosítva maradjanak.

A Google nyílt forráskódú implementációja ezt a két megoldást egyetlen protokollban egyesíti, lehetővé téve a közös adatpontokra épülő biztonságos számításokat. Ez a többlépcsős védelem olyan helyzetekben hasznos, ahol a felek szeretnének együttműködni, de az adatokat nem adhatják át egymásnak. Tipikusan ilyen terület az egészségügyi elemzés, a csalásfelderítés vagy a pénzügyi kockázati adatok összevetése. A Google hivatalos ismertetése szerint a PJC célja az, hogy az intézmények úgy tudjanak közösen statisztikákat készíteni, hogy közben adatvédelmi szempontból egyik fél se kerüljön kiszolgáltatott helyzetbe. A PJC előnye, hogy nem központi adatbázist épít, nem vonja össze a felek adatait, és nem „lát bele" azok tartalmába. A folyamat végén mindkét fél csak annyit tud meg,

amennyire ténylegesen szüksége van: például hány ügyfél közös a két intézmény között, vagy hogy milyen átlagérték jellemző az átfedésben szereplő rekordokra. Ez az adatvédelmi megközelítés biztonságosabb, mint a hagyományos adatmegosztási módszerek, mivel a teljes feldolgozás titkosított környezetben történik, és a nyers adatok egyszer sem kerülnek át egyik féltől a másikhoz (Walker et al. 2019).

A bankbiztonsági és biometrikus azonosítási folyamatokban a PJC különösen értékes olyan helyzetekben, amikor intézmények közötti egyeztetés szükséges – például csalási minták összevetésére, kockázatelemzésre vagy a hozzáférési jogosultságok összehangolására – úgy, hogy az intézmények közben nem adják át a saját adatbázisaikat.

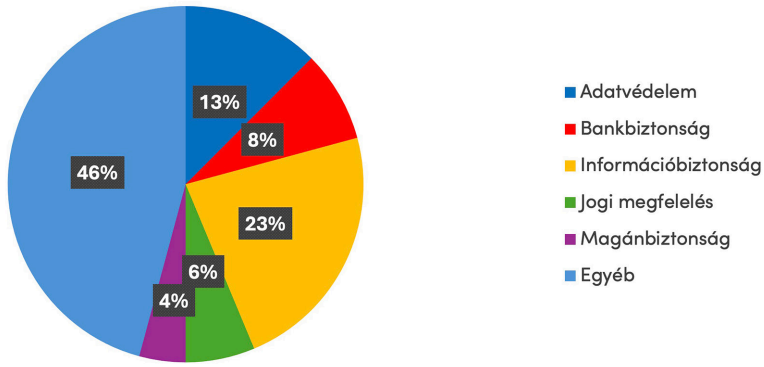
A kérdőíves kutatás eredményei ezzel összefüggésben arra utalnak, hogy a PJC-hez kapcsolódó kriptográfiai megoldások alkalmazása a jelentős adatvédelmi előnyök mellett konkrét technikai kockázatokat is hordoz. A válaszadók által jelzett aggályok között megjelent a megnövekedett számítási és erőforrásigény, valamint a skálázhatóság kérdése, különösen nagyméretű adatkészlet kezelése és intézmények közötti, ismétlődő adatkezelési műveletekkel járó együttműködések során.

Kiemelendő, hogy a titkosított számításokra épülő rendszerek biztonsága érzékeny a kriptográfiai paraméterek – így különösen a zajküszöb – megfelelő megválasztására. Amennyiben ezeket a paramétereket nem megfelelően állítjuk be, az a védelem gyengüléséhez, szélsőséges esetben a rendszer törhetőségéhez vezethet, miközben a paraméterezés a gyakorlatban nem tekinthető triviális feladatnak.

A PJC így olyan együttműködési lehetőségeket teremthet, amelyek korábban adatvédelmi okokból nem voltak biztonságosan megvalósíthatók, ugyanakkor a kutatás arra is rávilágít, hogy bankbiztonsági alkalmazása csak átfogó kockázatértékelés és megfelelő szakmai kompetencia mellett tekinthető fenntarthatónak.

Kutatási módszertan és a kérdőív bemutatása

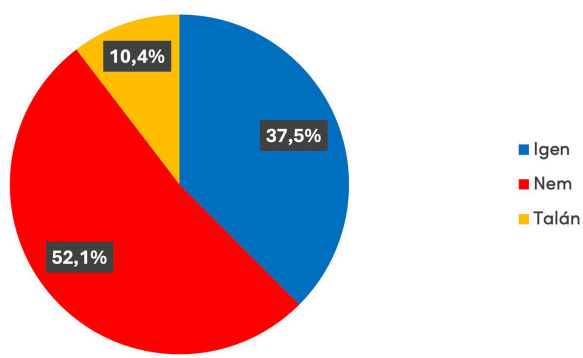
A primer kutatás egyik eleme a kérdőíves felmérés volt, amely a biometrikus azonosítással kapcsolatos adatvédelmi megoldások – különösen a homomorf titkosítás és a decentralizált adattárolás – szakmai elfogadottságát vizsgálta. Az adatfelvétel célzott, nem véletlenszerű szakértői mintavétellel történt, elsősorban bankbiztonsági, információbiztonsági, adatvédelmi és magánbiztonsági területen dolgozó szakemberek körében. A kérdőívet összesen 48 válaszadó töltötte ki. A felmérés 2025-ben zajlott, a kutatás lezárásáig. A válaszadók különböző szervezeti és biztonsági környezetet képviseltek, beleértve kritikus infrastruktúrát üzemeltető szervezeteket, kis- és középvállalkozásokat, valamint pénzügyi és technológiai területen működő intézményeket (1. ábra). A kérdőív 18 kérdésből állt, és elsősorban a technológiák ismertségére, gyakorlati alkalmazhatóságára, valamint az adatvédelmi és információbiztonsági kockázatok megítélésére fókuszált. Az így nyert adatok alkalmasak voltak a kutatási hipotézisek empirikus alátámasztására és a kvalitatív interjúk eredményeinek kiegészítésére.



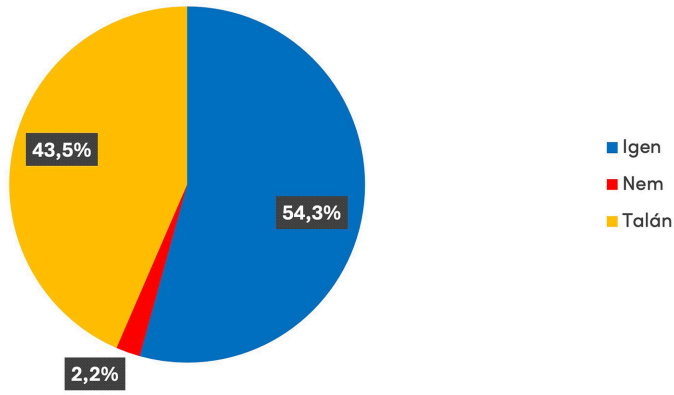
1. ábra: Foglalkozási területek
Forrás: a szerzők szerkesztése

Bankbiztonsági, információbiztonsági, adatvédelmi és magánbiztonsági szakemberek véleménye a homomorf titkosításról és a decentralizált adattárolásról

A válaszadók közül 47,9% hallott már a homomorf titkosításról (2. ábra), és közülük 97,8% úgy vélekedett, hogy ez a technológia potenciálisan alkalmazható a biometrikus adatok védelmére (3. ábra). Indoklásként többen kiemelték, hogy a homomorf titkosítás előnye, hogy a feldolgozási folyamat során nem szükséges visszafejteni az adatokat, ezáltal csökken az adatlopás vagy -szivárgás kockázata. Egyes válaszok szerint a homomorf titkosítás biztonságos adatmegosztást tesz lehetővé, amely különösen hasznos lehet pénzügyi környezetben, érzékeny ügyféladatok kezelése során.

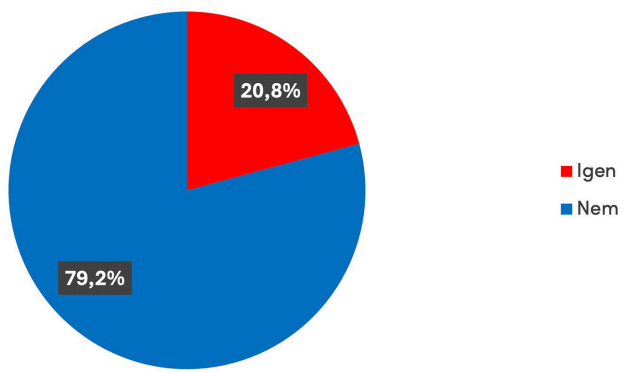


2. ábra: A homomorf titkosítás ismertsége
Forrás: a szerzők szerkesztése

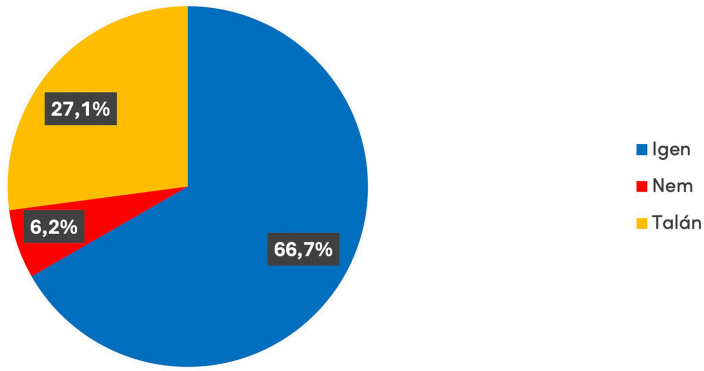


3. ábra: A homomorf titkosítás alkalmazhatósága
Forrás: a szerzők szerkesztése

A decentralizált adattárolást 79,2% ismerte (4. ábra), és 93,8% szerint (5. ábra) ez a tárolási mód növeli a biometrikus adatok védelmét. A válaszadók hangsúlyozták, hogy decentralizált rendszer esetén nem létezik egyetlen központi támadási felület, így az adatokhoz való jogosulatlan hozzáférés esélye jelentősen csökken.

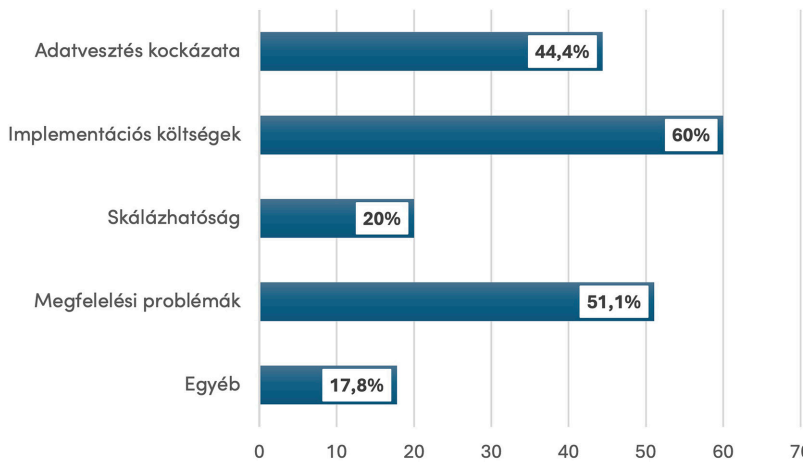


4. ábra: A decentralizált adattárolási megoldások ismertsége
Forrás: a szerzők szerkesztése



5. ábra: A decentralizált tárolás alkalmazhatósága
Forrás: a szerző szerkesztése

Ugyanakkor az aggályok között megjelent az adatvesztés kockázata, a skálázhatósági nehézségek és az implementációs költségek, valamint a megfelelési problémák is, amelyek technológiai és infrastrukturális szempontból további vizsgálatot igényelnek (6. ábra).



6. ábra: Aggályok
Forrás: a szerzők szerkesztése

Az adatvédelmi tisztviselők álláspontja

A kutatás kvalitatív módszertanra épült, amelynek során három adatvédelmi tisztviselővel készítettünk félig strukturált interjút, és az interjúk eredményeit a tartalomelemzés módszerével dolgoztuk fel. Az interjúalanyok kiválasztása célzott szakértői mintavétellel történt. Az interjúk eredményei egybehangzóan alátámasztják, hogy a biometrikus adatok különleges adatnak minősülnek, kezelésük kizárólag szigorú jogi és technikai feltételek teljesülése mellett tekinthető jogszerűnek.

A homomorf titkosítás kapcsán az egyik tisztviselő kiemelte, hogy ennek alkalmazása jelentősen csökkenti az adatlopás vagy adatszivárgás kockázatát, mivel nincs szükség a titkosított adatok visszafejtésére az azonosítási műveletek során. Ez a megállapítás közvetlenül megerősíti az első kutatási hipotézist.

A decentralizált adattárolással kapcsolatban elhangzott, hogy ez a megoldás csökkenti az adatbázisok sebezhetőségét, mivel megszünteti az egyetlen, központi támadási pontot. További érvként elhangzott, hogy a decentralizált rendszerek hozzájárulnak a felhasználói bizalom erősödéséhez, különösen olyan intézmények esetében, ahol magas szintű ügyfél-azonosításra van szükség. Míg az interjúalanyok eltérő mélységben és technikai részletességgel nyilatkoztak, mindannyian egyetértettek abban, hogy az adatvédelmi megfelelőség érdekében szükséges a biometrikus rendszerek átfogó kockázatértékelése és a korszerű kriptográfiai megoldások bevezetése.

Esettanulmányok a biometrikus adatok tárolásának sérülékenységéről

Az OPM ujjlenyomatadatainak kiszivárgása (Global Resilience Institute [é. n.])

2015-ben az Egyesült Államok Office of Personnel Management (OPM) adatbázisát ért kibertámadások során több mint 21 millió szövetségi alkalmazott személyes adata és 5,6 millió ujjlenyomat került illetéktelen kezekbe. A támadás jelentőségét tovább növelte, hogy az ujjlenyomatok egy része olyan pozíciókhoz kötődött, amelyek nemzetbiztonsági átvilágításhoz kapcsolódó dokumentációban szerepeltek. A Global Resilience Institute értékelése szerint az ujjlenyomatadatok kompromittálódása különösen súlyos, mert – a jelszavakkal szemben – ezek nem cserélhetők le, és így az érintettek számára élethosszig tartó biztonsági kockázatot hordoznak.

A jelentés azt is kiemeli, hogy a támadás hosszú távú következményei kiszámíthatatlanok, mivel az ujjlenyomatok más, későbbi azonosítási rendszerekben is felhasználhatók lehetnek. Az eset világosan rávilágít arra, hogy a nagyméretű központi biometrikus adatbázisok különösen vonzó és stratégiai jelentőségű célpontok, így védelmük nem csupán informatikai, hanem nemzetbiztonsági kérdés is.

Az amerikai CBP alvállalkozójának adatszivárgása (US Department of Homeland Security 2020)

2019-ben az amerikai vám- és határőrizeti szerv (Customs and Border Protection, CBP) egyik alvállalkozóját kibertámadás érte, amelynek következtében mintegy 184 000 utas

arcfelvétele és 105 000 rendszámtábla-felvétel került illetéktelen kezekbe. A Belbiztonsági Minisztérium Főfelügyelői Hivatalának jelentése szerint az incidens közvetlen oka az volt, hogy a vállalkozó nem tartotta be a CBP-szerződésben előírt adatbiztonsági követelményeket, többek között nem biztosította az adatok megfelelő titkosítását és hálózati elkülönítését. A vizsgálat arra is rámutatott, hogy a vállalkozó a szerződésben tiltott módon másolást és helyi adattárolást végzett, ami döntő szerepet játszott az adatok kompromittálódásában. A jelentés hangsúlyozza, hogy a biometrikus adatok kiszervezése a harmadik felek felé jelentős kockázatot hordoz, és az átlátható ellenőrzési, auditálási és incidenskezelési követelmények hiánya súlyos következményekhez vezethet.

Clearview AI elleni adatvédelmi eljárások (Office of the Privacy Commissioner of Canada 2021)

A Clearview AI arcfelismerő szoftvert fejlesztő vállalat ellen több nemzetközi adatvédelmi hatóság is vizsgálatot indított, miután kiderült, hogy a cég több milliárd nyilvánosan elérhető online képből hozott létre biometrikus adatbázist. A kanadai adatvédelmi biztos 2021-es jelentése szerint a Clearview AI hozzájárulás nélkül gyűjtött személyes adatokat, a gyűjtés célját nem határozta meg megfelelően, és a képfelhasználás módja sértette a kanadai személyes adatok védelméről szóló törvényt. A vizsgálat kiemelte, hogy a vállalat gyakorlata „erősen aránytalan beavatkozást" jelent az érintettek magánszférájába, mivel a képekből létrehozott biometrikus profilok akár az egyének mozgásának vagy online tevékenységének követésére is alkalmassá válhattak.

A Clearview AI más országokban is jogi következményekkel szembesült: az olasz adatvédelmi hatóság 2022-ben jelentős bírságot szabott ki, és megtiltotta az olaszországi adatgyűjtést, míg az Egyesült Királyság hatósága 2023-ban folytatta a jogorvoslati eljárást a vállalat ellen. Az eset jól mutatja, hogy a biometrikus adatok centralizált, kereskedelmi célú gyűjtése és tárolása nemzetközi szinten is súlyos adatvédelmi és jogi aggályokat vet fel.

Következtetések

A kérdőíves felmérés és az interjúk eredményei egyaránt megerősítik azokat a hipotéziseket, hogy a homomorf titkosítás és a decentralizált adattárolás nemcsak elméletileg ígéretes, hanem a gyakorló szakemberek által is támogatott, megvalósítható alternatíva a biometrikus adatok védelmére.

Az eredmények azt mutatják, hogy ezek a technológiák jelentős mértékben hozzájárulhatnak a pénzügyi szektor adatbiztonsági szintjének emeléséhez, miközben megfelelnek az adatvédelmi jogszabályok szigorú követelményeinek. A kutatás során nyert tapasztalatok és vélemények alapján kijelenthető, hogy az innovatív adatkezelési megoldások bevezetése mind szakmailag, mind társadalmilag indokolt és támogatott.

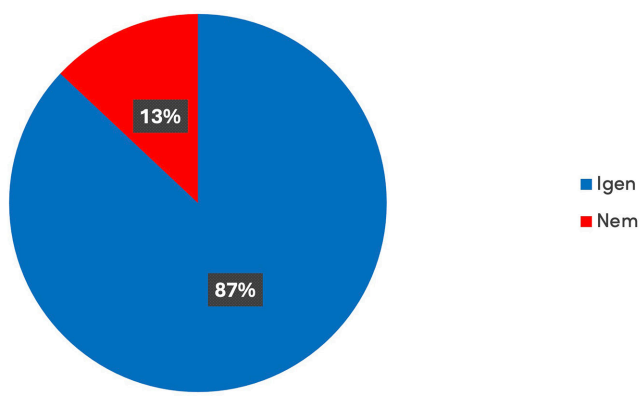
A kérdőív 18 kérdésének összegzése alapján a résztvevők többsége olyan munkaterületekről érkezett, ahol a biometrikus azonosításnak gyakorlati jelentősége van, és nemcsak nagy, hanem közepes és kisebb szervezetekben is komoly érdeklődés mutatkozik iránta. A legelterjedtebb azonosítási technológiák az ujjlenyomat- és az arcfelismerés, azonban az íriszazonosítás és

más megoldások még kevésbé használatosak. Az egyfaktoros azonosítás még mindig domináns, de a többfaktoros rendszerek iránti igény egyre nő. A válaszadók legnagyobb aggálya a személyes adatok védelme és a visszaélés lehetősége, különösen a nyers biometrikus adatok tárolása esetén. A jelenlegi védelmi rendszerek többnyire hagyományos IT-biztonsági megoldásokra épülnek, de a biometrikus adatok kezelésére nincs egységes, kifejezetten erre szabott védelem, ami új titkosítási és hozzáférés-kezelési módszerek bevezetését teszi szükségessé. A homomorf titkosítás ismertsége egyelőre alacsony, de a szakértők többsége lehetőséget lát benne, mert lehetővé teszi az adatok titkosított állapotban történő feldolgozását. Az adattárolásban a centralizált megoldások még elterjedtek, de a decentralizált és hibrid modellek iránti nyitottság növekszik, bár költséggel és implementációs kihívásokkal kapcsolatos fenntartások is vannak.

A válaszok egyértelműen jelzik, hogy a biometrikus adatok védelme fontos és kritikusabb, mint más adatoké, ezért a résztvevők többsége szerint új technológiákra és egyértelműbb szabályozási keretekre van szükség a teljes körű védelem biztosításához.

A válaszadók 87%-a egyetértett abban, hogy érdemes lenne a jogi szabályozást módosítani annak érdekében, hogy a homomorf titkosítást és a decentralizált adattárolást támogató innovációk könnyebben integrálhatók legyenek a gyakorlatba (7. ábra). Ez azt jelzi, hogy a szakmai közösség egységesen elismeri az új technológiák szerepét az adatbiztonság növelésében. A szakemberek nagy része nemcsak ismeri e technológiákat, hanem kifejezetten támogatja is azok alkalmazását a biometrikus adatok védelmére.

A vélemények komplexitása – a biztonságtechnikai előnyök és a gyakorlati korlátok párhuzamos megfogalmazásával – hozzájárul ahhoz, hogy a dolgozat kutatási kérdéseire megalapozott, árnyalt válaszok szülessenek.



7. ábra: A jogi szabályozás módosításának szükségessége
Forrás: a szerzők szerkesztése

A biometrikus azonosítás, az adatvédelem és a modern kriptográfiai megoldások kapcsolatának elemzése alapján egyértelműen kirajzolódik, hogy a biztonság jövője nem választható el az egyénhez kötött azonosítási módszerektől. A biometrikus technológiák – legyen szó

ujjnyomatról, íriszről, arcfelismerésről vagy viselkedésalapú jellemzőkről – olyan egyedi és stabil azonosítást tesznek lehetővé, amelyet korábbi módszerek nem tudtak elérni.

A bankbiztonsági kritikus szervezetek, infrastruktúrák területén különösen fontossá vált, hogy az azonosítás ne csak gyors és hatékony legyen, hanem másolhatatlan és megbízható is. Ez a biometrikus technológiák legfőbb előnye: a személy maga válik a kulccsá, amely minden korábbi hitelesítési konstrukciónál kevesebb támadási felületet hagy.

Ugyanakkor a biometrikus adatok természetéből fakadó sajátosságok olyan új adatvédelmi kihívásokat hoznak, amelyek az elmúlt évtizedben a GDPR egyik legszigorúbban kezelt területévé tették ezt a kategóriát. A biometrikus jellemzők elvesztése vagy kompromittálódása más, hagyományos azonosítókkal ellentétben nem korrigálható adminisztratív vagy technikai úton. Ez a tény hangsúlyt fektet arra, hogy a biometrikus rendszerek minden elemében a lehető legszigorúbb adatvédelmi és titkosítási elvek működjenek. A GDPR követelményeinek teljesítése és a biometrikus adatok biztonságos kezelése elvileg megoldható a hagyományos informatikai módszerekkel, azonban ezek a gyakorlatban csak részben biztosítják azt a garanciát, amelyre szükség van. A biometrikus sablonok titkosítása, az elkülönített tárolás, a hozzáférési protokollok és a rendszer-architektúra megtervezése ugyan növelik a biztonságot, de nem adnak valódi, matematikailag bizonyítható adatvédelmi garanciát. A konkrét fenyegetések – adattárak feltörése, belső visszaélések, biometrikus sablonok visszafejtésére irányuló támadások – rámutatnak arra, hogy a klasszikus titkosítási modellek önmagukban nem biztosítják a biometrikus adatok hosszú távú védelmét.

Ezen a ponton válik nélkülözhetetlenné a homomorf titkosítás és a decentralizált tárolási modellek integrációja. A homomorf titkosítás lehetővé teszi, hogy a biometrikus összevetés teljes folyamata titkosított adatokon menjen végbe: a rendszer egyetlen pontján sem kerül sor a nyers sablon vagy visszafejthető adat formájában történő hozzáférésre. Ez gyakorlatilag megszünteti a klasszikus adatlopás fogalmát a biometrikus rendszerekben, hiszen még sikeres támadás esetén is értékelhetetlen, matematikailag védett adathalmazhoz jutna hozzá a támadó. A decentralizált tárolás tovább erősíti ezt a modellt, mivel a sablonok több, egymástól független részegységben, eltérő struktúrákban és kulcsrendszerekben léteznek. Így nincs olyan kritikus pont, amelynek feltörése önmagában adatvédelmi incidenshez vezetne.

A három vizsgált terület – biometrikus technológia, adatvédelmi elvek és modern titkosítási megoldások – egymásra épülése komplex biztonsági architektúrát rajzol ki, és alkalmas a jövőbeni fenyegetések kezelésére. A biometrikus rendszerek biztonsága tehát már nem kizárólag a szenzorok pontosságán múlik, hanem azon, hogy a teljes adatkezelési lánc a gyűjtéstől a feldolgozásig és tárolásig milyen titkosítási és elosztási módszerekkel működik. A jövő biometrikus rendszerei nem egyszerű hozzáférési megoldások lesznek, hanem kifejezetten kriptográfiai rendszerek, amelyek matematikai bizonyíthatóságon alapuló garanciákat nyújtanak.

Jövőbeli irányok

A bankbiztonsági rendszerek fejlesztése során olyan irányok kijelölése indokolt, amelyek a biometrikus azonosítást, a homomorf titkosítást és a decentralizált adattárolást egységes, egymást erősítő keretrendszerbe rendezik. A biometrikus azonosítás banki ügyfél-azonosításban betöltött szerepe tovább fog erősödni, és a következő években olyan mértékű integráció várható, amely a jelenleg alkalmazott jelszavas vagy okmányalapú hitelesítést fokozatosan háttérbe szorítja. A fejlődés sebességét a technológiai érettség, az infrastruktúra-képességek és a szabályozói elvárások együtt határozzák meg, ezért a banki rendszereknek már most olyan fejlesztési irányokat kell követniük, amelyek hosszú távon is fenntarthatók és skálázhatók.

A homomorf titkosítás olyan stratégiai, jövőbe mutató eszközzé válhat, amely képes teljesen új szintre emelni a biometrikus adatok feldolgozásának biztonságát. A titkosított adattal végzett műveletvégzés lehetőséget teremt arra, hogy a biometrikus sablonok soha ne kerüljenek visszafejtett formában a rendszerhez, így az azonosítási folyamat minden pontja védett maradjon. A banki gyakorlatban érdemes olyan architektúrák kialakítására törekedni, amelyek a biometrikus összehasonlítást és a hitelesítési logikát teljes mértékben titkosított környezetben képesek végrehajtani.

Bár a technológia jelenleg még jelentős erőforrásokat igényel, a hardveres gyorsítók és optimalizált algoritmusok megjelenése a közeljövőben lehetővé teszi a széles körű alkalmazást.

Az elosztott, *blockchain* alapú adattárolás beemelése a biometrikus rendszerekbe a jövő bankbiztonsági stratégiáinak egyik központi eleme kell legyen. A decentralizált modellek olyan védelmi szintet biztosítanak, amelyben a jogszerűtlen hozzáférés az egyes csomópontokhoz nem teszi lehetővé az adatok manipulálását vagy tömeges eltulajdonítását. Ennek megfelelően ajánlott olyan hibrid struktúrák megtervezése, ahol a központi infrastruktúra stabilitása kiegészül a *blockchain* rendszerek hamisíthatatlanságával és elosztott ellenálló képességével. Bár ez nem egyik napról a másikra megvalósítható átállás, hosszú távon jelentősen csökkenti a banki biometrikus adatvagyon koncentrált támadási felületeit.

A szabályozói környezet várható alakulása szintén meghatározza a fejlesztési irányokat. A GDPR, a NIS 2 és a hazai kiberbiztonsági előírások jelenleg is magas szintű megfelelési követelményeket támasztanak, de a biometrikus technológiák gyors ütemű fejlődése indokolttá teszi ezek további szigorodását. A banki szektor számára célszerű olyan protokollokat és belső működési elveket kialakítani, amelyek rugalmasan követik a szabályozói változásokat, és már előre beépítik a következő években várható kötelező titkosítási, auditálási és adattárolási előírásokat. A biometrikus azonosítás csak akkor válhat hosszú távon is megbízható biztonsági megoldássá, ha a rendszerbe épített titkosítási és adattárolási megoldások garantálják, hogy a biometrikus adatok illetéktelen szereplők számára ne legyenek hozzáférhetők. Ezt a védelmi szintet a teljesen titkosított feldolgozási modellek – különösen a homomorf titkosítás –, valamint a decentralizált adattárolási architektúrák együttes alkalmazása képes megteremteni. A technológiai eljárásoknak ugyanakkor illeszkedniük kell a magas szintű etikus adatkezelési elvekhez és a szabályozási környezet követelményeihez, hogy a biometrikus rendszerek hosszú távon biztonságosan, átláthatóan és a banki működés egészét támogató módon fejlődhessenek tovább.

Felhasznált irodalom

Albrecht, Martin et al. (2018): *Homomorphic Encryption Security Standard*. Online: https://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf

Biographical sketch, John Daugman [é. n.]. Online: https://www.cl.cam.ac.uk/~jgd1000/bio-sketch.html

Chripko, Agnes (2025): How Accurate Is Walking Recognition? Uncovering the Precision of Our Technology. *Cursor Insight,* 2026. február 2. Online: https://www.cursorinsight.com/post/1900/how-gait-recognition-is-becoming-a-digital-fingerprint

Csaba Zágon – Tóth Attila (2024): A Magánbiztonsági és Önkormányzati Rendészeti Tanszék tíz éve tudományos publikációkban. *Magyar Rendészet,* 24(6), 145–162. Online: https://doi.org/10.32577/mr.2024.ksz.10

Gentry, Craig (2009): *A Fully Homomorphic Encryption Scheme.* Disszertáció. Stanford University. Online: https://crypto.stanford.edu/craig/craig-thesis.pdf

Global Resilience Institute [é. n.]: *5.6 Million Fingerprints Stolen in OPM Data Breach.* Online: https://globalresilience.northeastern.edu/5-6-million-fingerprints-stolen-opm-data-breach/

Grother, Patrick – Salamon, Wayne – Chandramouli, Ramaswamy (2013): *Biometric Specifications for Personal Identity Verification.* [H. n.]: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-76-2

Jain, Anil K. – Nandakumar, Karthik – Ross, Arun (2016): 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters,* 79, 80–105. Online: https://doi.org/10.1016/j.patrec.2015.12.013

Lippai Zsolt – Mezei József (2024): Gondolatok a magánbiztonsági szektor humánkockázat-kezeléséről. *Nemzetbiztonsági Szemle,* 12(1), 18–35. Online: https://doi.org/10.32561/nsz.2024.1.2

Office of the Privacy Commissioner of Canada (2021): *PIPEDA Findings #2021-001: Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*. Online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

Szabó Máté Dániel (2004): Biometrikus azonosítás és adatvédelem. *Acta Humana,* 15(1), 81–92.

Tiszolczi, Balázs G. (2023): Biztonságtechnikai rendszerek védelme, biztonságos üzemeltetése. In Gyaraki Réka (szerk.): *Az információbiztonság alapjai.* Budapest: Nemzeti Közszolgálati Egyetem, 113–180. Online: https://doi.org/10.37372/mrttvpt.2023.3

Trauring, Mitchell (1963): Automatic Comparison of Finger-Ridge Patterns. *Nature,* 197(4871), 938–940. Online: https://doi.org/10.1038/197938a0

Ujhegyi Péter (2023): A biometria elterjedésének elemzése. *Belügyi Szemle,* 71(8), 1463–1491. Online: https://doi.org/10.38146/BSZ.2023.8.7

Ujhegyi Péter – Kun Tamás (2020): Adatkezelés mesterfokon – a biometrikus azonosítás és a jogszabályi háttér. *Biztonságtudományi Szemle,* 2(3), 13–30. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/75

US Department of Homeland Security (2020): *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot (OIG-20-71).* Online: https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf

Walker, A. et al. (2019): Helping Organizations Do More Without Collecting More Data. *Google Online Security Blog,* 2019. június 9. Online: https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html

Felhasznált jogszabályok

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

Szabvány

ISO/IEC 24745:2022(en) Information Security, Cybersecurity and Privacy Protection – Biometric Information Protection