ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

BÁLINT KRISZTIÁN

Személyazonosításra alkalmas automatizált elektronikus blokklánc kialakítása

Témavezető: Prof. Em. Dr. Berek Lajos

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 202… hónap nap

Szigorlati vizsga bizottság:

Elnök:

Prof. Dr. Rajnai Zoltán

Tagok:

Dr. Szűcs Endre

Dr. habil. Berek Lajos

Nyilvános védés teljes bizottsága:

Nyilvános védés időpontja:

202... hónap nap

TARTALOMJEGYZÉK

Munkámat családomnak ajánlom

"Talán különös dolog ilyet mondani, de egyedül a fejlődésben, az átalakulásban és a változásban találhatjuk meg az igazi biztonságot."

Anne Morrow Lindbergh

BEVEZETÉS

A XXI. században az informatika gyors fejlődésének köszönhetően a biztonsági kamararendszerek az oktatási intézményekben is széleskörűen elterjedtek. Ezeket leggyakrabban a hallgatók és az ott dolgozók biztonsága érdekében telepítik. A kamerák a „hagyományos megfigyelés” mellett a jövőben olyan feladatokat is elláthatnak, amelyeket ez idáig senki sem valósított meg. Ilyen lehet a hallgatói jelenléti ívkészítő kamerarendszer, amely a biztonság fokozása érdekében az adatokat a felhő helyett a blokkláncban tárolja el. Ez egyedülálló megoldásnak számít napjainkban. A tudományos kutatásomban ezért egy ilyen rendszer létrehozását mutatom be.

Napjainkban a biztonsági kamerák már komoly, akár 4K képes felbontással rendelkeznek, beépített mesterséges intelligencia támogatása mellett. A nagy felbontás lehetővé teszi a pontos arcérzékelést, arcfelismerést, valamint létszám megállapítást, amely elengedhetetlen az automatizált elektronikus jelenléti ívkészítés során.

Ahhoz, hogy a jelenléti ív létrejöhessen a kamerának olyan adatbázissal kell, hogy rendelkezzen, amely pontosan ismeri a hallgatók órarendjét, illetve a tantermek beosztását. Ilyen típusú azonosítás esetében az adatbázisbiztonság kiemelt fontosságú kell, hogy legyen, mivel érzékeny hallgatói adatok tárolásáról van szó. A még biztonságosabb adattárolás érdekében létrehoztam egy saját egyetemi ÓUDSC (Óbudai University Data Storage Chain, Óbudai Egyetem adattároló blokklánc) nevű blokkláncot, amelyhez kizárólag az oktatási intézménynek van hozzáférése.

Továbbá a rendszer nem titkolt célja az egyetemi adminisztratív munka megkönnyítése. Az Óbudai Egyetem Hallgatói Követelményrendszerének Tanulmányi és Vizsgaszabályzata határozottan megköveteli a hallgatóktól a tanórák rendszeres látogatását, ezért a jelenléti ív alkalmazására szükség van. A személyazonosításra alkalmas blokklánc alapú jelenléti ívkészítő rendszer ebben nyújt nagy segítséget, mivel a rendszer alkalmazása által az oktatókat tehermentesíti a tanórák alatt, így nem kell a hallgatói jelenléti ívvel foglalkozniuk, helyette a tényleges oktatásra koncentrálhatnak. Nem mellesleg a környezetvédelmet is szem előtt tartva kevesebb papírmunkára van szükség a fentebb vázolt digitális megoldás alkalmazása által.

Nem utolsó sorban pedig a személyazonosításra alkalmas jelenléti ívkészítő rendszer a tűzvédelemben is kamatoztatható. A kamera mivel képes a hallgatók pontos helyzetét meghatározni, ezért ezt a tudást az evakuáció során is megálja a helyét. Így egy esetleges gyors

kimenekítés során az élőerős védelem pontos információkkal rendelkezhet arról, hogy az összes hallgató elhagyta-e az oktatási intézményt.

Az automatizált hallgatói jelenléti ívkészítő rendszer alkotóelemei a következők:

- Mesterséges intelligenciával rendelkező biztonsági kamera,
- NVR (Network Video Recorder, Hálózati videórögzítő) egység,
- Saját egyetemi ÓUDSC nevű blokklánc,
- Okosszerződés,
- Egyetemi napló, illetve hagyományos levelező rendszer.

A tudományos kutatásomban a személyazonosításra alkalmas jelenléti ívkészítő rendszer létrehozásának lépéseit mutatom be.

A kutatási téma időszerűsége

A mindennapi életünkben gyakran előfordul egy a számunkra igen fontos kategória a biztonság. [1]

A biztonság iránti igény mindig is fontos szerepet játszott. A technológia gyors fejlődésének köszönhetően napjainkban olyan modern elektronikai megoldások is a rendelkezésre állnak, amely néhány évtizeddel ezelőtt még elképzelhetetlenek voltak. A biztonsági kamerák nem csak az objektumvédelemben, hanem az élet számos területén mindig is fontos szerepet játszanak. Hasznosságukat hosszasan lehetne sorolni.

Az utóbbi években az oktatási intézményekben is megjelentek a biztonsági kamerák, amelyek nem csak az ott dolgozók, hanem a hallgatók biztonságát is hivatottak növelni. A kamerák elsődlegesen megfigyelő feladatokat látnak el. [2], [3]

Az analitikai funkciók megjelenésével és a mesterséges intelligencia alkalmazásával, azonban a felhasználható hatékonyságuk jelentősen megnövekedett. A már rendelkezésre álló analitikai funkciókat figyelembe véve időszerű elgondolkodni azon, hogy hogyan lehetne ezeket a tulajdonságokat még inkább az oktatási intézmény javára fordítani? Milyen hozzáadott tudás által lehetne még hatékonyabbá tenni azokat az oktatási intézmény falain belül? Figyelembe véve az összes rendelkezésre álló analitikai funkciót, érdemes ezeket együttesen alkalmazni, abból a célból, hogy a kamerarendszer képes legyen jelenléti ívet készíteni a hallgatók óralátogatásáról. Ez által egy olyan személyazonosításra alkalmas jelenléti ívkészítő rendszert hozok létre, amely minden bizonnyal előremutató megoldásnak számít, hiszen éppen a digitalizáció korában

mutatkozik a legnagyobb igény a technikai újdonságok iránt. E lehetőséget kihasználva, nem csak tovább fokozható a biztonság a precízebb hallgatói azonosítás érdekében, hanem egyes rutinszerű napi feladatokat is automatizálhatóak, úgy, mint a hallgatói jelenléti ívkészítés.

Az adatbázisbiztonság is időszerű téma, ezért a kamerarendszer az adatokat már nem a „hagyományos felhőben" tárolja el, mivel azok kompromitálódása az utóbbi években már bebizonyosodott. Ilyen nagyobb eseményekről még a média is beszámolt. Ezen okból a kamerarendszer a blokkláncban tárolja el az adatokat, amellyel a tudományos világ még csak most ismerkedik. A blokkláncok a különböző csomópontoknak köszönhetően nagyobb adatbiztonságot garantálnak. Ebben az esetben egy bonyolult megoldásról van szó, mivel az NVR egységet össze kell kapcsolni a blokklánccal. Újdonság, hogy lehetőség függvényében az oktatási intézmény akár saját blokkláncot is létrehozhat, ez által ő szabályozhatja a különböző adattárolási jogosultságokat a teljes rendszer felett.

Nem utolsó sorban a kamerarendszer a tűzvédelemben is hatékonyan alkalmazható, így egy olyan komplex biztonsági rendszert alakítható ki, amely példaértékűnek számít a felsőoktatási intézmények esetében. Mivel a kamera képes a hőérzékelésre, ezért tűz esetén riaszt. Ezt a tulajdonságot kibővítve azzal, hogy a személyazonosításra alkalmas jelenléti ívkészítő rendszer ismeri a hallgatók nevét és pontos tartózkodási helyét egy olyan komplex kamerarendszeren alapuló tudásbázis jöhet létre, amely előremutató megoldásnak számít a tudományos jövőt illetően.

A kutatási téma és a biztonságtudomány kapcsolata

A biztonság iránti igény mindig is fontos szerepet játszott az emberek életében. Biztonságról általában akkor szoktak beszélni, amikor valamilyen veszélyeztető tényező is fennáll. Az emberi élet védelme mindig is fontos szempont volt, hiszen ki ne szeretné a saját családját, gyermekét biztonságban tudni? Már az őskorban is a férfi védelmezte a családját, otthonát. Ennek érdekében különböző szerszámokat készített és szükség esetén alkalmazta is azokat. A biztonságtechnika fejlődésével újabbnál újabb eszközök jelentek meg, amelyek már nem csak az otthon védelmét szolgálták, hanem az élet számos területét is lefedték.

A megfelelő biztonság érdekében védelmi erőforrásokat célszerű alkalmazni. Megkülönbözetünk technikai jellegű erőforrásokat és élőerőst. A technikai kategóriába tartozik a mechanikai,

elektronikai és a személyek által alkalmazott eszközök. [1] Fontos megjegyezni, hogy az élőerő kiemelt fontosságú a védelmi eszközök szakszerű használatában.

Az iskolai biztonsági megoldások hatalmas fejlődésen mentek keresztül az utóbbi évtizedben. Az elektronikai védelem részeként megjelentek a biztonsági kamerák és a beléptetőrendszerek. Ezek mind az egyetemen tartózkodók biztonságát hivatottak szolgálni, abból a célból, hogy oda illetéktelen ne tudjanak bejutni. A jelenléti ívkészítésre alkalmas biztonsági kamerák szorosan kapcsolódnak azon biztonságtechnikai törekvésekhez, mely által növelni lehet az iskolai biztonsági szintet. A kamerák analitikai tudása előremutató megoldás az elektronikus iskolai védelemben. Az előerő munkáját nagyban támogatja, mivel beléptetéskor képes a hallgatók név szerinti azonosítására.

Az elektronikus tűzjelző rendszer az elektronikai vagyonvédelem részét képezi. Az automatikus tűzjelző rendszer képes a tűz érzékelésére és jelzésére. Tűz esetén riaszt még a tűz fejlődésének kezdeti szakaszában. Ez által a nagyobb anyagi károk elkerülhetőek. [1]

A biztonságtechnikai megoldásokat széleskörűen alkalmazva a jelenléti ívkészítő kamerarendszer képes a tűzjelzésére és észlelésére az oktatási intézmény falain belül. Beépített hő szenzorai akár egy kezdődő tüzet is képesek időben észlelni. Az arcfelismerő és létszám meghatározó funkcióinak köszönhetően az evakuáció során az oktatási intézményben tartózkodók mozgása is hatékonyabban nyomon követhető.

Napjainkban megnövekedett a vagyon és az információ védelmének a lehetősége, [1] ezért a kamerarendszer az adatok biztonságos tárolása érdekében blokklánc technológiát használ. A blokkláncban az adatok kevésbé vannak kitéve a kompromitálódás veszélyeinek, ezért az nagyobb biztonságot nyújt, mint más nagyvállalatotok felhőszolgáltatásai. A blokkláncban a hallgatók óralátogatásaival kapcsolatos adatok és a biztonsági felvételek kerülnek mentésre, amely érzékeny adatoknak minősülnek.

Tudományos probléma megfogalmazása

A tudományos probléma egy olyan kérdés, vagy feladat, amelynek megválaszolását nem lehet azonnal megtenni. [4] A tudományos probléma felvetéseit ezért kutatási kérdésekkel fogalmazom meg.

Kutatásom során a modern biztonsági kamerák tudását olyan módon próbálom kiaknázni, hogy azok az oktatási intézményekben még hatékonyabbá váljanak, illetve, hogy még több feladat ellátására legyenek képesek.

Tudományos problémaként fogalmazódik meg egy olyan személyazonosításra alkalmas hallgatói jelenléti ívkészítő rendszer létrehozása, amely a biztonsági kamerák segítségével képes felismerni és azonosítani a hallgatókat, valamint azokról automatizált módon naprakész jelenléti ívet hoz létre. Oktatói szempontból ez azért fontos, mivel a rendszer alkalmazása által a jelenléti ív készítése teljesen automatizálható, ez által csökkenteni lehet a tanórai adminisztrációs terheket, valamint a hallgatók óralátogatása is könnyebben nyomon követhető. Hallgatói szempontból azért fontos, mivel a papíralapú jelenléti ív kitöltése idő igényes feladat, amely a tanórákból értékes perceket képes elrabolni, így a hallgatóknak több idejük marad a tananyag elsajátítására.

A rendszer adottságait kihasználva képessé válik arra, hogy az elektronikai tűzvédelem részét is képezze, mivel a hallgatók mozgását folyamatosan képes nyomon követni, így az evakuáció során a „eltévedt” hallgatók rövid időn belül kimenekíthetőek. Az adatok biztonságos tárolása érdekében a rendszer blokklánc technológát alkalmazva az érzékeny adatokat egy saját egyetemi blokkláncba tölti fel. Ennek a jelenléti ívkészítő rendszernek a létrehozását egyrészt azért találom fontosnak, mivel a tudományos életben ez idáig ilyen komplex rendszert még nem valósítottak meg, nem utolsó sorban pedig a jelenléti ívkészítő rendszer csökkenti a csalás, valamint visszaélés lehetőségét.

Témaválasztás indoklása

Kutatásom tárgyának a “A személyazonosításra alkalmas automatizált elektronikus blokklánc kialakítása” témát választottam, mivel ez idáig informatika tanárként dolgoztam és érdekelnek a modern technikai megoldások.

A doktori képzésem alatt folyamatosan kutattam a felsőoktatási intézményekben alkalmazott biztonságtechnikai megoldásokat, úgy Magyarországon, mint Szerbiában.

Informatikusként mindig is érdekeltek az olyan technikai lehetőségek, amelyek által bizonyos dolgokat jobbá, tökéletesebbé lehet tenni. Ezért a már rendelkezésre álló ismeretanyagomat próbáltam elmélyíteni és egy olyan automatizált elektronikus hallgatói jelenléti ívkészítő rendszert megalkotni, amely által a biztonsági kamerák alkalmassá válnak hallgatói jelenléti ívkészítésére.

Már az általános iskolai tanári pályafutásom során is adott volt a lehetőség arra, hogy betekintést nyerjek a tanári munkába, elsajátítsam a pedagógiai módszereket és megfigyelhessem a napi szinten alkalmazott biztonságtechnikai megoldásokat.

Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában számos biztonságot érintő témakörrel foglalkoztam. A tudásomat próbáltam az elektronikai védelemi megoldások terén elmélyíteni. Ezért kidolgoztam egy olyan biztonsági kamerákon alapuló jelenléti ívkészítő rendszert, amely által a hallgatók biztonságát hatékonyan lehet növelni, ezzel párhuzamosan pedig az oktatókra nehezedő adminisztrációs terheket csökkenteni.

A belgrádi Singidunum Egyetem közgazdasági szakán a blokklánc technológiával foglalkoztam, azon belül is annak lehetséges iskolai alkalmazásával, ebből kifolyólag a már rendelkezésemre álló ismeretanyagomat fejlesztettem tovább. A blokklánc technológia alkalmazása által adott a lehetőség arra, hogy az oktatási intézmény biztonsági kameráit összekapcsoljam az intézményi adminisztrációs rendszerrel, amely által a jelenléti ívkészítése automatizált módon jöhet létre.

Az Óbudai Egyetem Trefort Ágoston Mérnökpedagógiai Központban mesterszakon okleveles mérnöktanári diplomát szereztem, ahol részleteiben megismerkedtem az egyetemi adminisztrációval és számos olyan ehhez kapcsolódó feladattal, amely a tanárokra nehezedik nap mint nap. Továbbá a Singidunum Egyetem informatikai mesterszakon Korszerű információs technológiákból diplomatám, ahol különböző informatikai rendszerekről szereztem ismeretanyagot.

Általános iskolai mentortanárként mindig felhívtam a gyakorlatot teljesítő hallgatók figyelmét arra, hogy az óra elején szigorúan ellenőrizzék a jelenlévők névsorát, a hiányzókat pedig maradéktalanul írják be a naplóba. Mivel ebben az esetben kiskorúakról volt szó, ezért erre külön figyelmet fordítottam. Ha az általános iskolában dolgozó tanár tévesen igazol egy hiányzást, mivel nem veszi észre, hogy hiányzik a tanuló az órájáról és közben a diákkal történik egy „baleset” akkor a tanár lesz a felelős.

Jelenleg az Óbudai Egyetem Keleti Károly Gazdasági Szakán tanársegédként dolgozok, ahol úgyszintén informatikát tanítok. A felsőoktatásban nem használatos az általános iskolai napló, helyette minden órán hallgatói jelenléti ívet kell készíteni a hallgatók hiányzásairól, amelynek függvényében megkaphatják a szemeszter végén az aláírást. 10 éves munkatapasztalat távlatából

kijelenthetem, hogy hallgatói jelenléti ív alkalmazása nélkül nem ajánlatos órát tartani. Ezért a kutatásomban ennek a rutinszerű folyamatnak az automatizálását próbálom megvalósítani biztonsági kamerák által.

Az eddig megszerzett tudásomra, illetve tanulmányaimra alapozva választottam a témát, hiszen ez a megoldás jelenleg újdonságnak számít napjainkban a digitalizáció korában.

Célkitűzések

Céljaim megfogalmazása során meghatároztam a kutatásom legfontosabb irányvonalait, más szóval a célkitűzésekkel az elérni kívánt eredményeket vetítettem előre. [5]
Kutatásom elsődleges célja volt megvizsgálni, hogy a biztonsági kamerák analitikai funkciói képesek-e felismerni és azonosítani a hallgatókat, ugyanis ez elengedhetetlen a személyazonosításra alkalmas elektronikus jelenléti ív elkészítéséhez. További kutatási célként a blokklánc technológiában rejlő lehetőségeket vizsgáltam, mivel egy saját egyetemi blokklánc létrehozásával és okos szerződés megírásával a hallgatók adatait automatizált módon képes elmenteni a rendszer a blokkláncba.

Kutatásom további célja volt megvizsgálni, hogy az automatizált személyazonosításra alkalmas blokklánc alapú jelenléti ívkészítő rendszer képes-e a hallgatók arcképeihez időbélyeget rendelni a csalás és visszaélés elkerülése érdekében.

Kutatási célként vizsgáltam, hogy a személyazonosításra alkalmas jelenléti ívkészítő rendszer alkalmazható-e az egyetemi elektronikai tűzvédelem részeként.

Célom volt továbbá, hogy empirikus kutatási módszerek segítségével elemezzem, majd feltárjam azt, hogy a hallgatók esetében okoz-e tanulási nehézséget, illetve frusztrációt a folyamatos megfigyelésre és azonosításra alkalmas jelenléti ívkészítő rendszer.

Végül, de nem utolsó sorban kutatásom céljaként felmértem az oktatók véleményét a személyazonosításra alkalmas elektronikus blokklánc alapú jelenléti ívkészítő rendszer egyetemi alkalmasságáról.

A téma kutatásának hipotézisei

- **Hipotézis 1**

  Feltételezhető, hogy létrehozható egy olyan hallgatói jelenléti ívkészítő rendszer, amely a biztonsági kamerák segítségével képes felismerni és azonosítani a hallgatókat és a blokklánc technológia segítségével azokról automatizált módon jelenléti ívet tudna készíteni.

- **Hipotézis 2**

  Feltételezhető, hogy az automatizált hallgatói jelenléti ívkészítő rendszer csökkenti a csalás, valamint visszaélés lehetőségét.

- **Hipotézis 3**

  Feltételezhető, hogy a jelenléti ívkészítő rendszer alkalmazható az elektronikai tűzvédelemben az evakuáció során. Ez a rendszer képes lenne arra, hogy a hallgatók mozgását nyomon kövesse, így tűz esetén az „eltévedt" hallgatók a lehető legrövidebb időben belül kimenekíthetőek.

- **Hipotézis 4**

  Feltételezhető, hogy a folyamatos megfigyelésre és azonosításra alkalmas automatizált biztonsági kamerákon alapuló jelenléti ívkészítő rendszer a hallgatókat nem feszélyezi az oktatási intézményben és hasznos megoldásnak találják annak mindennapos alkalmazását.

- **Hipotézis 5**

  Feltételezhető, hogy az egyetemi oktatók a személyazonosításra alkalmas elektronikus blokklánc alapú jelenléti ívkészítő rendszert hasznos megoldásnak találják az oktatási intézményekben, mivel így automatizált módon készíthetnek jelenléti ívet a hallgatók óralátogatásáról.

A technológia és a kutatások jelenlegi állása, kutatásom helye a világban

A tudományos kutatásomban számos olyan technológiai megoldással foglalkoztam, amelyek újdonságnak számítanak napjainkban. Meglátásom szerint a kutatások során mindig célszerű a lehető legújabb rendelkezésre álló technológiákat megvizsgálni és lehetőség függvényében azokat tovább fejleszteni. Az automatizált elektronikus hallgatói jelenléti ívkészítő rendszer létrehozása egy igencsak bonyolult folyamat, mivel egymástól teljesen új és független technológiai megoldásokat kell egymással összekapcsolni a cél elérése érdekében. A jelenléti ívkészítő rendszer a legújabb biztonsági kamera és blokklánc technológiákat öleli fel.

A kutatás újdonság erejének következtében ez idáig kevés tudományos munka jelent meg a témakörökben. Ez alatt értendő a blokklánc technológia, azon belül is az, amely az adattárolással foglalkozik. Értelemszerűen minden blokklánc képes az adatok tárolására, azonban ezek kis mennyiségű adatok. A nagy felbontású kamerarendszerek viszont hatalmas adatmennyiséget generálnak, amely tárolását meg kell oldani. A biztonság további fokozása érdekében azonban nem csak az adat tárolása szükséges a blokkláncban, hanem célszerű egy saját egyetemi blokkláncot is létrehozni. Ilyen esetben az oktatási intézmény határozhatja meg a blokklánc működésének szabályait. A blokklánc technológiával jelenleg ismerkedik a világ, az abban rejlő lehetőségek még nincsenek kihasználva. A kutatásom során a rendelkezésre álló tudományos munkák nagy részét ezekben a témakörökben áttekintettem. Megállapítottam, hogy sem Magyarországon sem Szerbiában az oktatási intézmények nem használnak blokklánc technológiát. A kutatási témához kapcsolódó alábbi újdonságok jelentek meg ez idáig:

- Egyes középiskolákban arcfelismerésre képes kamerák figyelik a diákok viselkedését. Különböző viselkedésmintákat képesek felismerni, úgy mint, írás, olvasás, jelentkezés, tanárra figyelés. [6]
- Az egyetemek saját blokklánc létrehozása után akár okos szerződéseket is köthetnek a hallgatóikkal. A blokklánc az oktatásban betöltött szerepe alapján képes a hallgatók érdemjegyeit figyelemmel kísérni a Neptun rendszeren keresztül. Ez egy új ösztöndíj kifizető megoldás, amely teljesen automatikus módon működik. A hallgatóknak vállalniuk kell az okos szerződés keretében azokat a kötelezettségeket, amelyek az ösztöndíj kifizetéshez szükségesek. Ilyen lehet a jeles érdemjegy a félév, illetve az év végén. Amennyiben a hallgató megszerzi a szükséges érdemjegyeket, úgy a rendszer azokat észlelve bárminemű adminisztrátori beavatkozás nélkül elutalja a havi ösztöndíjat. E lehetőség alkalmazása által tehermentesíteni lehet az oktatási intézményeket. [7]
- A biztonságos adattárolás érdekében megjelentek a decentralizált megoldások, amelyek blokklánc technológián alapulnak. Ez sokkal nagyobb biztonságot nyújt, mint a felhőalapú megoldás. [8]
- Egyes kutatások szerint az okos városokban az érzékeny adatok mentése a blokkláncokban kerülnek majd rögzítésre. A térfigyelő biztonsági kamerák felvételei itt tárolódnak majd el, mivel a blokklánc alapú főkönyv biztosítja azt a lehetőséget, hogy az adatok nem

kompromittálódhatnak. Ezen oknál fogva a felvételeket feltételezhetően a bíróságok bizonyítékként el fogják fogadni, mivel azok megegyeznek a valósággal. [9]

- Továbbá számos egyetem kutatja annak a lehetőségét, hogy az egyetemi diplomákat ne csak papíralapon adják ki, hanem elektronikus formában is, amelyeket a blokkláncban tárolnának el. Az amerikai MIT (Massachusetts Institute of Technology) Egyetem ezt a lehetőség aktívan teszteli. Erre azért lenne szükség, mivel nem egy esetben előfordult már, hogy a jelentkezők a munkáltatóknak hamis diplomákat nyújtottak be. [10]

Egyetemi kutatások folynak arról, hogy a felsőoktatási intézmények hogyan tudnának saját blokklánc rekordokat létrehozni, amelyben a hallgatók óralátogatásaival, illetve tandíj befizetésével kapcsolatos információkat tárolnának. A blokkláncok többségében a rekordokat nem lehet módosítani, így azok megfelelő biztonságot nyújthatnak. Amennyiben mégis hibásan rögzítenének adatokat a rekordban, akkor egy új rekordot kellene létrehozni. A blokklánc struktúrájából adódóan a régi és az új rekord is látható maradna, azonban az új javított rekord válna a releváns rekorddá. [11]

A jelenléti ív megvalósításához mesterséges intelligenciával rendelkező kamerarendszerek használatára is szükség van, méghozzá olyanokra, amelyek teljes mértékben kihasználják a már rendelkezésre álló analitikai funkciók nagy részét. Első lépésként ezeket a funkciókat vizsgáltam, hogy képesek-e felismerni a hallgatókat? A technológia jelenlegi állása szerint a válasz az, hogy igen, erre adott a lehetőség, azonban a tudomány ezzel a témakörrel még nem foglalkozott. Ezen felül a mai modern biztonsági IP kamerarendszereket össze lehet kapcsolni a blokklánccal az NVR egység segítségével. Az automatizáció, a biztonság és a hatékonyság növelése érdekében a blokklánc és a kamerarendszer közé ajánlatos egy okos szerződést beépíteni, amely az adatok tárolásával kapcsolatos feladatokat látja el. A tudományos világban ez idáig ilyen komplex egymástól függetlenül működő rendszereket még nem kapcsoltak össze abból a célból, hogy automatizált módon hozzanak létre hallgatói jelenléti ívet az oktatási intézmények számára.

A kutatás felépítése

A kutatásom a következő struktúra szerint épült fel. A bevezetés után a kutatási témám időszerűségét vizsgáltam. Erre azért mutatkozott szükség, mivel számos kutatási területet érint a témám, úgy, mint a modern analitikai kamera funkciókat, a blokklánc technológiát és okos

szerződéseket is, így célszerű volt ezeknek a témáknak az időszerűségét és aktualitását megvizsgálni.

A célkitűzések fejezetben meghatároztam az elérni kívánt eredményeket. Elsősorban megvizsgáltam azt, hogy milyen lehetőségek adottak a hallgatói jelenléti ívkészítés megvalósításához. Célom volt egy biztonságos adatbázis létrehozása, ahol a jelenléti ívvel kapcsolatos adatokat tudtam eltárolni. További célkitűzésként a szerbiai egyetemi hallgatók és oktatók véleményét is feltártam a jelenléti ívkészítő rendszerről.

Ezt követően megfogalmaztam a kutatásom hipotéziseit. Vizsgáltam továbbá a kutatásom helyét a világban és azt is, hogy a jelenléti ívkészítő rendszer a tudományos életben milyen szerepet tölt be.

A kutatásom első nagyobb témája a modern biztonsági kamerarendszerek témaköre volt, amely során a biztonsági kamerák tudását vizsgáltam. Kutattam a biztonsági kamerák specifikus tulajdonságait, úgy, mint a beépített mesterséges intelligenciát, valamint vizsgáltam a rendelkezésre álló képfelbontást és a videó tömörítési algoritmusokat. Mivel a jelenléti ívkészítő rendszer a tűzvédelem részét képezheti, ezért a biztonsági kamerák hőérzékelő tulajdonságait is megvizsgáltam.

Ezt követően a blokklánc technológiát kutattam, azon belül is a blokklánc struktúrát és annak felépítését. Megvizsgáltam a nyilvános és privát blokkláncban rejtőző lehetőségeket abból a célból, hogy megtaláljam a lehető legoptimálisabb blokklánc megoldást, amellyel a jelenléti ívkészítő rendszer összekapcsolható.

Részleteiben áttekintettem az adattárolási megoldásokat. Ezt több részre bontottam, mivel az adatok elsődleges tárolása az NVR merevlemezén történt. Ezek a tárolási architektúrák fontos szerepet töltenek be az adatbiztonság szempontjából. Ide tartozik a DAS (Direct Attached Storage - Közvetlenül csatolt tárolás), NAS (Network Attached Storage - Hálózatra csatolt tároló), SAN (Storage Area Network - Tároló hálózat), RAID (Redundant Array of Independent Disk - Tárolási technológia) és az iSCSI (Internet Small Computer Systems Interface - Internet SCSI tárolóhálózat) megoldás. Ezt követően az adatok hosszútávú tárolási lehetőségét is kutattam. Ilyen a decentralizált és centralizált adattárolási megoldás. Míg az utóbbi megoldásról számos esetben kiderült, hogy nem nyújt kellő védelmet, addig a decentralizált megoldás egyre inkább előtérbe

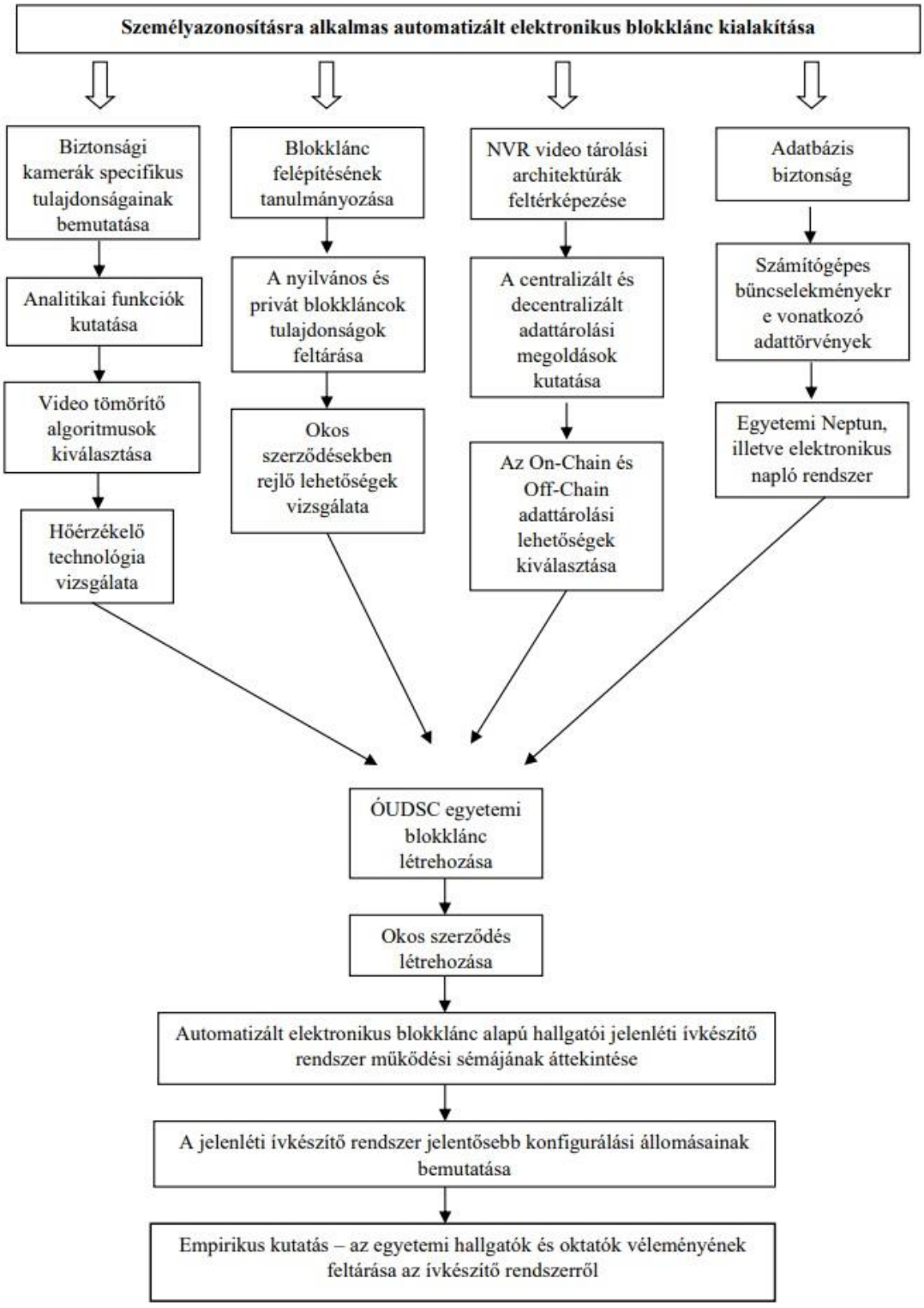
kerül az informatika fejlődésével. Megvizsgáltam mindkét decentralizált adattárolása megoldást, úgy az On-Chain, mint az Off-Chain blokkláncokat.

Kutatásomban az adatbázis-biztonsággal is foglalkoztam. Kutattam a lehetséges oktatási intézményeket fenyegető adatbázis veszélyeket. Részleteiben kitértem a videókamerák által készített felvételek Európai Uniós, magyarországi és szerbiai szabályozásaira és törvényeire.

A gyakorlati megvalósításom során létrehoztam az ÓUDSC nevű egyetemi blokkláncot. Bemutattam továbbá az ÓUDSC blokklánc struktúrát és a jelenléti ív működésének sémáját. Ezt követően definiáltam az okos szerződésben az előre meghatározott szerződési feltételeket. Kiemeltem a jelenléti ívet készítő rendszer fontosabb konfigurálási állomásait és leírtam a rendszer tűzvédelmi működésének sémáját. A gyakorlati megvalósítás során a tapasztalataimat megosztottam. A jelenléti ívkészítő rendszer megalkotása során számos akadály és probléma felmerült. Kitértem az NVR egység konfigurálása során felmerült problémákra. A kamerák tesztelése során komoly problémát jelentett a generált adatok nagy mennyisége. Leírtam, hogy ezeket az akadályokat, hogyan sikerült megoldanom.

A gyakorlati megvalósítás után empirikus kutatási módszerekkel megvizsgáltam a hallgatók és az oktatók meglátását a jelenléti ívkészítő kamerarendszerről.

Kutatásom lezárasaként összefoglaltam a disszertációm munkáját. Megfogalmaztam az elért új tudományos, valamint az empirikus kutatásom során kapott eredményeimet, nem utolsó sorban pedig a kutatásom folytatásának lehetséges irányvonalait vázoltam fel. Az alábbi ábra a disszertációm logikai felépítését mutatja be.



1. ábra. A disszertációm logikai felépítése

1 BIZTONSÁGI KAMERARENDSZEREK

A biztonsági kamerák az élet minden egyes területén jelen vannak, úgy a munkahelyeken, mint a parkokban és a forgalmas úthálózatokon. Napjaink modern nyugati nagyvárosaiban nem lehet úgy végig haladni, hogy egyetlenegy biztonsági kamera látószögébe se kerüljön az ember. Kiszámolták, hogy már kétezres évek elején Londonban egy átlagos embert nem kevesebb mint 300-szor filmez le mintegy 30 különböző videó hálózat. [12]

Az első videó megfigyelésre alkalmas kameráknak számos hátrányuk volt. Nagy részük csak nappal készített elfogadható felvételeket. Az adatok tárolása sem volt hatékony, hiszen a felvételeket videókazettára, illetve videószalagra rögzítették. [13]
A biztonsági kamerák fejlődése szorosan kapcsolódik a televízió és a film készítés történetéhez.

- Az első filmkamera Thomas Edison és William Dickson feltaláló nevéhez fűződik. 1893-ban mutatták be az első nyilvános mozgóképet. Ez után kezdték el készíteni az első filmeket, amely később a biztonsági kamerák megjelenéséhez vezetett.
- 1939-ben jelent meg az első úgynevezett miniatűr kamera, amelyet akár egy kézben is lehetett tartani. Ettől az időponttól kezdve vált lehetővé a rejtett kamerás megfigyelés a történelem során. [14]
- Az időben bő két évtizedet visszaugorva 1913-ban már a londoni börtönőrök is próbálkoztak a megfigyelésre szolgáló fényképezőgépek használatával információgyűjtés céljából. Titokban felvételeket készítettek a rabokról.
- 1942-ben megjelent a CCTV (Closed-Circuit Television - Zártláncú videó megfigyelő rendszer) amelyet Németországban használtak először ballisztikus rakéták biztonságos megfigyelésére. A rendszer két kamerából állt, amely a rakéták indítását figyelte.
- Az Egyesült Államokban 1949-ben az első ipari CCTV rendszert elkezdték forgalmazni, így az szélesebb kör számára elérhetővé vált. Koaxiális kábellel lett összekötve a kamera a monitorral, amely 525 soros felbontást használt. Ez a maga idejében igencsak előremutató megoldásnak számított.
- 1956-ban a Hamburgi német rendőrség elkezdte az utcákra telepíteni a kamerarendszert, melynek célja a lakosság biztonságérzetének a növelése volt.
- 1990-ben az ATM-ekbe (Automated Telles Machine - Bankautomata) elkezdték beépíteni a biztonsági kamerákat.

- 1996-ban megjelent az IP (Internet Protocol – Internet protokoll) kamera, amely képes információk küldésére és fogadására a hálózaton keresztül.
- 2020-ban a Covid vírussal fertőzött beteg emberek szűrése is lehetővé vált. A kamera az emberek testhőmérsékletének figyelése is képes. A megengedett érték felett riaszt. [15]

Megállapítható, hogy a technika gyors fejlődésének köszönhetően a biztonsági kamerákra egyre nagyobb igény mutatkozik az élet számos területén. [16]

1.1 Biztonsági kamerarendszerek tulajdonsága (kamerákról általánosságban)

A biztonsági kamerák széleskörű elterjedésének köszönhetően az élet számos területén lehet velük találkozni nap mint nap. Elsődleges feladatuk éveken át a biztonság növelése, illetve a már meglévő biztonsági szint fokozása volt megfigyelés által. Ez azonban a kétezres években jelentősen megváltozott, mivel a beépített analitikai funkcióknak köszönhetően, úgy, mint az létszám megállapítás, arcfelismerés, elhagyott tárgy észlelése hozzáadott értékeket képviselnek. A továbbiakban már nem célszerű úgymond „passzív" eszközként tekinteni rájuk. Az intelligens biztonsági kamerák hozzájárulnak a felvételek kiértékeléséhez és analizálásához. A mesterséges intelligencia nélküli kamerák általában a videóadatok 10%-át használják fel, míg a modern kamerák akár az adatok 100%-át is képesek analizálni. Minden adatot megfigyelnek a felvételen, ez által a fontosabb történésekről szinte azonnali visszajelzést adnak. Ezek a kamerák képesek adatokat továbbítani nem csak a felvevő egység irányába, hanem olyan adatbázisok felé is, amelyek adatgyűjtést, illetve értelmezést végeznek további információ kinyerése céljából. [17]

Többek között a következő helyeken alkalmazzák a biztonsági kamerákat:

- Beléptető rendszerek kiegészítésére,
- Áruházakban, boltokban, bevásárlóközpontokban,
- Pénzintézetekben,
- Oktatási intézményekben,
- Közúti közlekedésben,
- Vállalati létesítményekben,
- Repülőtereken,
- Országhatárok védelmében.

Az analitikai funkcióval felvértezett kamerák úgynevezett intelligens algoritmussal rendelkeznek. Ezek az algoritmusok a mesterséges intelligencia által megtanulják az egyes viselkedésmintákat felismerni. Ezek a következők lehetnek:

- Gyanús viselkedés. Ilyen lehet, ha valaki fegyvert vesz elő, vagy éppen mozdulatlan,
- Tárgyak elhagyására is riaszthat a kamerarendszer. Pályaudvarokon, repülőtereken, múzeumokban ezek a funkciók hasznosak lehetnek,
- A zsebtolvajlást, bolti lopásokat nehéz időben észrevenni, de egy jól „betanított" kamera számára ez nem marad rejtve,
- Az emberek mozgás közbeni azonosítása sem megoldhatatlan feladat a mesterséges intelligenciát alkalmazó kamerák számára. [18]
- Megfigyelhető, hogy az oktatási intézmények is egyre gyakrabban telepítenek biztonsági kamerákat, hiszen az áruk folyamatosan csökken, míg a tudásuk folyamatosan növekszik. Egy esetleges lopás, különböző iskolai normaszegések a kamerák által könnyen nyomon követhetőek, az utólagos bizonyítás is sokkal egyszerűbbé válik.

1.2 Biztonsági kamerák felbontása

A mai modern biztonsági kamerák felbontása leggyakrabban a HD (High Definition – Nagyfelbontás) kategóriába esik, amely igencsak részletgazdag felbontást eredményez már nagyobb távolságból is. Egy képfelbontást többféle képen meg lehet adni. Két általános gyakorlat létezik erre. Ezek a következők:

- A vízszintes, illetve a függőleges képpontok számának a meghatározása, valamint a
- Megapixelek meghatározása (például: 1 megapixel = 1 millió képpont).

A jelenléti ívkészítő rendszer megalkotása során a kamerák felbontásának a kiválasztása jelentőségteljes feladat volt. Nyilvánvalóan nem mindegy, hogy a kamera milyen felbontással rendelkezik, hiszen a nagyobb felbontásnak köszönhetően jelentősen javulhat a képminőség is.

Ezen felül fontos különbséget tenni az IP kamerák, illetve a hagyományos analóg kamerák között. Mind a két kameratípusnak megvan a maga előnye, illetve hátránya.

Az IP kamerák saját maguk végzik el a digitalizációt, tehát maguk alakítják képpontokká az általuk látott valóságot. Ahhoz, hogy a kamerák képfelbontása ne csökkenjen, megfelelően kiválasztott NVR egységre is szükség van. Az IP kamerák esetében a beágyazott hardvereknek és az azokon

futó szoftvereknek köszönhetően digitálisan előállított kép kerül tömörítésre és egyben kódolásra is. Ezután már átvihető egy IP protokollon (pl. Ethernet) keresztül és a digitális jelsorozat rögzítésre kerülhet mind a kamerában, mind a hálózati rögzítő egységen (NVR). [19]

Az egyetemek esetében az IP kamerák számos olyan plusz lehetőséget biztosítanak, amely fontosak lehetnek az oktatási intézmény számára. Ezek a következők:

- Nincsen szükség minden egyes kamerát kábellel összekötni a felvevő egységgel.
- Nagyobb képfelbontással rendelkeznek.
- Kibővített analitikai funkciókat használnak a hagyományos kamerához képest.
- Alkalmas lehet az online jelenléti ívkészítésre is.

1.3 A megfelelő videótömörítési algoritmus kiválasztása

Minél részletgazdagabb és hosszabb egy videófelvétel, az annál nagyobb adatmennyiséget jelent. A biztonsági kamerák fejlődésével a megapixel-ek (MP – Megapixel - Felbontóképesség) száma is arányosan növekedett, ezáltal a rögzíteni kívánt adatok is egyre több helyet foglaltak el az NVR merevlemezén. Természetesen még ilyen esetben az adatok megfelelő tárolásáról gondoskodni kell. Ilyen lehet a nagyobb merevlemezek beszerzése, valamint azok tárolása távoli szervereken. Ez mind olyan feladat, amelyet előre meg kellett terveznem a rendszer megvalósításánál.

A személyazonosításra alkalmas jelenléti ívkészítő rendszer esetében a generált adatok mennyiségére külön figyelmet kellett fordítanom, ezért az adatmennyiség csökkentése érdekében megvizsgáltam a rendelkezésre álló videó tömörítési algoritmusokat. Ezek a következők voltak:

- MJPEG (Motion Joint Photographic Experts Group - Mozgókép tömörítási eljárás),
- H.264,
- H.265.

Az egyik legismertebb tömörítési eljárás a JPEG (Joint Photographic Experts Group), amelyet széleskörűen alkalmaznak. Használata által hatékonyan lehet a képi fájlok méretét csökkenteni. Jellemző rá, hogy amit egyszer JPEG-be formátumba átalakítottak, az bizonyos szintű minőségveszteséget szenved el. [20]

A Motion JPEG tömörítési eljárás során minden egyes képkocka JPEG formátumra tömörítődik és ezek a képkockák fűződnek össze egy egységes videó folyammá. Előnye, hogy alacsony a

számítógép igénye, így gyengébb paraméterekkel rendelkező számítógépeknél, illetve digitális felvevőegységeknél is jól használható. Jellemzően az 5:1-es tömörítési arány esetében még viszonylag jó minőségű képet lehet kapni, míg a 10:1-es arány során már észrevehető a képromlás. [21]

Jellemzően 16 fps (kép/másodperc) sebesség mellett a mozgásban levő képeket már videónak lehet érzékelni. Ez azonban igen alacsony érték. Az MJPEG a 30 kép/másodperc értéket általában problémamentesen tudja tartani még gyengébb felvevőegységek esetében is. Mivel minden kép JPEG minőségű, ezért a videó minősége várhatóan megfelelő lesz. [22] A megfigyelőrendszerek esetében széleskörűen alkalmazzák, azonban a médiapiacon kevésbé terjedt el, mivel a hanginformációt nem tudja tömöríteni. [23]

A H.264/AVC szabvány az MPEG2-hez viszonyítva 50%-al sikerült javítani. [24] A H.264 akár 80%-al képes csökkenteni fájl méretét a Motion JPEG-hez képest. A szabvány alkalmazása előtt gyakran előfordult, hogy a biztonsági kamerák esetében csökkentették a felbontás részletességét a digitális adattárolás korlátai miatt. Ez leginkább a 4MP kamerákra volt jellemző, mivel már a Full HD (Full High Definition – Teljes nagyfelbontás, 1080p) felbontás is részletgazdag videófelvételt biztosított a 2592x1520 felbontás helyett. Az alkalmazott módszer hátránya, hogy ez által a biztonsági kockázat növekedett. [25]

A H.265 a H.264 utódja, amelyből az következik, hogy a tömörítési hatékonyságot sikerült tovább növelni. A HEVC (High Efficiency Video Coding – Nagy hatékonyságú videoó tömörítés) működésének a lényege olyan területek keresése a képkockán, amelyek redundánsak, tehát nem változnak. Amennyiben ilyen területeket talál a tömörítési eljárás, úgy csak a hivatkozást menti el. A blokkok mérete a H.264 esetében 16x16 pixelesek, míg a HEVC alkalmazásakor sokkal kisebbek 64x64 pixelesek. Ez precízebb tömörítést tesz lehetővé. [26]

A videó tömörítő algoritmusok elemzése után arra a következtetésre jutottam, hogy a személyazonosításra alkalmas jelenléti ívkészítő rendszer esetében a H.265 szabvány alkalmazásával tudom a leghatékonyabban csökkenteni az adatmennyiséget, ezért a gyakorlati megvalósítás során ezt fogom használni.
Az alábbi első táblázatban a különböző tömörítési eljárásokat mutatom be a generált adatmennyiség figyelembevétele mellett:

Felbontás	Tömörítési eljárás	Kamerák száma	Napok száma	Napi órák száma	Szükséges hálózati sávszélesség	Adat-mennyiség
1.3MP (HD)	Tömörítés nélkül	24	5	12	16Gbit/s	497TB
1.3MP (HD)	MJPEG	24	5	12	873 Mbit/s	24TB
1.3MP (HD)	H.264	24	5	12	145 Mbit/s	4016GB
1.3MP (HD)	H.265	24	5	12	130 Mbit/s	3613GB
2MP (1080p)	Tömörítés nélkül	24	5	12	27 Gbit/s	787TB
2MP (1080p)	MJPEG	24	5	12	1.35Gbit/s	38TB
2MP (1080p)	H.264	24	5	12	230 Mbit/s	6354GB
2MP (1080p)	H.265	24	5	12	177 Mbit/s	4904 GB
10 MP	Tömörítés nélkül	24	5	12	135 Gbit/s	3811TB
10 MP	MJPEG	24	5	12	6.6 Gbit/s	185TB
10 MP	H.264	24	5	12	1.1 Gbit/s	31TB
10 MP	H.265	24	5	12	858 Mbit/s	24TB

1. táblázat. Biztonsági kamerák különböző tömörítési eljárásainak hatékonysága [27], [28]

Mint látható egy 24 kamerából álló rendszerrel kalkuláltam, amely heti öt napot működik. A tanítás jellegéből adódóan kijelenthető, hogy az oktatás általában reggel 8h és este 20h közötti időintervallumot ölel fel, amely 12 órás folyamatos kameraműködést jelent. Amennyiben hétvégen is zajlik oktatás, úgy ez az adatmennyiség növekedni fog. Megállapítottam, hogy a legnagyobb

adatmennyiséget a 10 MP kamerák generálják tömörítés nélkül, valamint, hogy az oktatási intézményeknek célszerű a H.265 szabványt választaniuk, mivel nagy hatékonysággal képes adatokat tömöríteni. Ez elengedhetetlen a jelenléti ívkészítés során.

1.4 A kamera mesterséges intelligenciája - analitikai funkciók

Az optimális pixelfelbontás és videó tömörítési algoritmus kiválasztása után a kamerák analitikai funkcióit is megvizsgáltam. Az analitikai funkciók többsége mesterséges intelligenciát használ. Ez által a kamera folyamatosan tanul, felismeri és értékelni tudja a különböző helyzeteket, így csökkentve a téves riasztások számát. A mesterséges intelligenciával ellátott kamerák minél hosszabb ideig működnek (napokon, heteken vagy akár hónapokon keresztül), annál hatékonyabbakká válnak, így a hallgatókat sokkal precízebben tudják azonosítani. A rendszer nem titkolt célja, hogy a hallgatókat hatékonyan azonosítsa. Hibás azonosítás során előfordulhat, hogy a rendszer nem regisztrálja a hallgatót, így őt akár hiányzónak is elkönyvelheti, holott a tanórán részt vett. Ebből akár kellemetlen helyzet is keletkezhet, így az analitikai funkciókon nagyon sok múlik.

Ahhoz, hogy kamera képes legyen elkészíteni a hallgatói jelenléti ívet a következő analitikai funkciókkal kell, hogy rendelkezzen:

- Arcérzékelés,
- Arcazonosítás,
- Létszám megállapítás,
- Arcadatbázis,
- Mesterséges intelligencia. [29]

Az analitikai funkció a kamera mesterséges intelligenciájának részét képezik. A kutatásom megvalósítása során a gyakorlatban olyan biztonsági kamerákat kellett választanom, amelyek tartalmazzák a fentebb felsorolt összes funkciókat, mivel kizárólag azok együttes alkalmazásával lehet elkészíteni a jelenléti ívet. Amennyiben ezek közül egy is hiányzik, úgy az automatizált online jelenléti ív nem jön létre.

1.4.1 Arcérzékelés

Az ember számára az arc felismerése nem okoz problémát, azonban a biztonsági kamerák számára ez egy igencsak összetett feladat. Minél nagyobb képfelbontással rendelkezik a kamera, annál hatékonyabban tudja az arcot érzékelni. [30]
Ez természetesen nem elegendő a sikeres arc érzékeshez, ezen felül beépített mesterséges intelligenciára és számos analitikai funkcióra is szükség van.

Az arcfelismerést az arcérzékelés előzi meg. Az arcdetektálás segítségével a kamera automatikusan felismeri az emberi arcot, valamint hatékonyan elkülöníti azt a többi testrésztől. Az arcdetektálás során a vizsgálat tárgyát képezi a:

- Fejforma,
- Az arc részleteinek geometriája,
- Bőrszín.

Az automatikus arcdetektálást nehezítő tényezők lehetnek:

- Részlegesen eltakart arcok (ez lehet szándékos takarás, illetve véletlen),
- A fej pozíciója (elfordítva vagy szemből nézve),
- Részletgazdag, strukturált háttér. [31]

A gyakorlatban az AdaBoost tanulóalgoritmus által, amelyet Paul Viola és Michael Jones szerzőpáros fejlesztett ki, a kamera hatékonyan tudja az emberi arcot felismerni. A módszer alapját a téglalap alakú régiókból képzett jellemzők alkotják. A legtöbbet alkalmazott módszer a két téglalapos régiók egyszerre történő vizsgálata. Az egyik régió az eredeti, míg a másik az integrált képet vizsgálja a detektor segítségével. A detektort három fő része lehet bontani. Ezek a következők:

- Integrálkép létrehozása,
- Osztályozók tanítása AdaBoost-alapú tanulóalgoritmussal,
- Az osztályozók kaszkádstruktúrába építése. [32]

1.4.2 Arcazonosítás

Az arcbiometriát széles körben alkalmazzák, úgy, mint mobiltelefon-hitelesítés, határ és vámkezelés, rendőrségi azonosítások alkalmával. A csalók azonban mindent megtesznek, hogy

megnehezítsék az azonosítást, illetve, hogy tevésen azonosítsák őket. A modern kamerarendszerek ezeket a metaadatokat megpróbálják hatékonyan kezelni, valamint ezen hibalehetőségeket lecsökkenteni. [33]

A mai modern kamerarendszerek a csalás elkerülése céljából két különféle fókuszban elkészített képet használnak bemeneti képként. Ezzel a módszerrel könnyen kiszűrhetőek a nagyfelbontású 2D-s nyomtatott képek, mivel a valódi és a hamis arcok között eltérő a mélységi információ. A módszer lényege, hogy kamera a szem, orr, fül, illetve száj közötti távolságot is figyelemmel kíséri. [34]

Az oktatási intézményekben az arcfelismerési technológia egyre inkább elterjed. Pár évvel ezelőtt kizárólag biztonsági megfontolásból telepítettek kamerákat, addig napjainkban az automatikus regisztráció, valamint a hallgatók érzelmeinek észlelése is előtérbe került. Habár az arcfelismerésből fakadó vitákban az iskolák ritkán szerepelnek, ennek ellenére nem szabad elfelejteni, hogy lehet, hogy ez az a hely, ahol a hallgató először találkozik folyamatos monitorozással. Az arcfelismerő technológia képes kinyerni a videófelvételre mentett arcjellemzőket, amelyeket összehasonlít az adatbázisban elmentett arcokkal. Érdemes tudatában lenni annak, hogy az arcfelismerés nem olyan pontos, mint az íriszfelismerés, vagy az ujjnyomat azonosítás, [35] ennek ellenére sokkal gyorsabb azoknál. Ez előnyös lehet, ha a gyors azonosítás elsődleges szempont, mivel a hallgatókat minden egyes tanóra előtt azonosítani kell a tantermek bejárata előtt. Az iskolai arcfelismerés előnye a többi biometrikus azonosításhoz képest a:

- Távoli azonosítás,
- Gyorsaság,
- Egyszerre több hallgató felismerése,
- Passzív részvétel az azonosításban, mivel elegendő a kamera előtt elhaladni.

Hátrányként fogalmazható meg:

- Ha több hallgató egymást takarva megy be a tanterembe,
- Túl kontrasztos háttér,
- A hallgatók szándékosan takarják az arcukat,
- Az arcfelismerő algoritmus nem megfelelő működése.

1.4.3 Létszám megállapítás

Ahhoz, hogy az létszám megállapítást az oktatási intézményben az NVR sikeresen el tudja végezni dupla lencsés (dual-lens) kamerákra van szükség. Az egy lencsés kamerák az embereket tévesen azonosítják, így azok számos tárgyat is emberként észlelnek. A változó látási viszonyok, illetve az árnyékok is negatívan hatnak ki az emberszámlálásra. Ezzel szemben a dupla lencsés kamerák két képet készítenek egyszerre a személyről, létrehozva a háromdimenziós képet. A módszer lényege, hogy pontosan felmérje az emberek egyes paramétereit, úgy, mint a magasságukat és az alakjukat. [36]

Az online jelenléti ívkészítő kamera esetében a létszám megállapítás egy nagyon hasznos analitikai funkció, amelyet az oktatási intézményben a következő helyeken javasolt alkalmazni:

- Az egyetem bejáratánál. Ez által az iskolavezetés pontosan meg tudja határozni az oktatási intézményben tartózkodó hallgatói létszámot. Egy esetleges tűzeset során a biztonsági szolgálatnak, valamint a kiérkező tűzoltóknak is hasznos információval szolgál.
- A tantermekben bejárati ajtaja előtt. A hallgatók azonosítása mellett a kamerarendszer a tanteremben tartózkodó hallgatók létszámáról is pontos információval rendelkezik, továbbá az arcfelismerő technológiának köszönhetően név szerint képes azonosítani a hallgatót. Ez által egy komoly és megbízható biztonsági rendszer valósítható meg.

1.4.4 Arcadatbázis

A biztonsági kamerák funkciójaként az arcadatbázis az utóbbi években széleskörűen elterjedt, amelyet számos biztonsághoz kapcsolódó területen használnak napjainkban. Ezek a következők:

- Az útlevelek ellenőrzésekor rendszeresen alkalmazzák a hatóságok,
- A rendvédelmi szervek a gyanúsítottak ellenőrzésekor,
- Gyanús szervezetek és cégek esetében (ilyen lehet az adócsaláshoz kapcsolódó tevékenységek),
- Kaszinótulajdonosok és fogadóirodák is alkalmazzák ezt a módszert.

Kártékony számítógépes programok, illetve vírusok esettében is hasznos tud lenni eme sajátos tulajdonságokkal rendelkező adatbázis. [37]

A személyazonosításra alkalmas jelenléti ívkészítő rendszer esetében az arcadatbázis egy olyan sajátos adatbázist takar, amely alapján könnyedén ki lehet szűrni az illetéktelen személyeket. Amennyiben olyasvalaki próbál bejutni egy megfigyelt területre, ahova nincsen jogosultsága, úgy a kamera riasztja az élőerős védelmet. Alkalmazása által a beléptetőrendszert kiegészítve hatékonyan lehetne növelni a már kialakított biztonsági szintet. Míg a beléptetőrendszer esetében a biometrikus azonosításhoz aktív részvételre van szükség, addig a biztonsági kamera passzív részvétel alapján működik. E két rendszert kombinálva jelentősen csökkenthető annak az esélye, hogy illetéktelen személy jusson be az intézménybe az élőerős védelem, illetve a portai szolgálat tudta nélkül.

1.4.5 Mesterséges intelligencia

Az emberi arc számos információval rendelkezik, amelyet a mesterséges intelligenciának már az azonosítás előtt fel kell dolgoznia. Először is meg kell találni az ember arcát, valamint követni azt a mozgása során. A hatékonyság érdekében ezt valós időben kell elvégeznie. Késedelemnek ilyen esetben nincsen helye, mivel, ha valaki már elhaladt a kamera látószöge előtt és nem történt meg az azonosítás, rosszabb esetben az érzékelés, úgy a rendszer értelmét veszti és a biztonság hiányossá válik. Jelenleg a biztonsági kamerák másodpercenként 2-3 alkalommal tudják végrehajtani a felismerést. [38]

A jelenléti ívkészítő kamerarendszer mesterséges intelligenciával kell, hogy rendelkezzen. A hallgatói arcfelismerés során számos probléma jelentkezhet, amelyet a kamerának meg kell tudnia oldani. Ezek a következők:

- Az arckifejezés felismerése:
  - Akár egy mosoly is kihathat az arc vonalaira, mivel megváltoztathatja azt.
  - Különböző érzelmi állapotok is kihatnak az arci jellemzőkre. Ilyen lehet: (harag, depresszió, szomorúság, boldogság, undor, szégyen, megvetés, szorongás). [39]
- Takarás:
  - Arcjegyek teljes/részletes takarása más objektumok által.
  - A tanterembe való belépéskor a hallgatók akár véletlenül is takarhatják egymást.
- Képminőség:
  - A tantermek fényviszonya, megvilágítása, valamint sötétítés és árnyékolás.

- Tantermek színe, különböző tárgyakról való fényvisszaverődés (ez leginkább a laborokra jellemző).

- Arcjegyek megléte, illetve hiánya:
  - Haj nagysága, haj színe, arcbőr színe.
  - Szakáll, bajusz, tetoválás. [40]

1.5 Hőérzékelős kamerák

Az oktatási intézményeket kötelezően fel kell szerelni tűzjelző rendszerekkel és érzékelőkkel. Ezt a törvény is előírja. Az elektronikus tűzjelző rendszer tűz esetén érzékel, jelez és riaszt, ezzel csökkentve az anyagi károkat. A legfontosabb azonban az emberi élet megóvása, ahol kulcsfontosságú a tűz kezdeti szakaszában történő riasztás. A következő tűzjelző rendszereket különböztetjük meg:

- Hagyományos hurkos kialakítású,
- Címzett hurkos kialakítású,
- Analóg intelligens,
- Interaktív tűzjelző. [1]

Az úgynevezett „hagyományos” érzékelők mellett a hőérzékelésre képes kamerákat is ajánlatos alkalmazni az oktatási intézményekben, ezzel is növelve a tűvédelem biztonsági szintjét. A hőkamera minden olyan anyagot észlel, amely melegebb, mint az abszolút nulla fok. Azok a tárgyak, amelyek ettől melegebbek, elektromágneses sugarat bocsájtanak ki infravörös tartományban, amelyet az emberi szem képtelen észlelni, de a kamera ezeket jól látja. Azért, hogy az emberi szem számára ez látható legyen, a kamera hőmérsékleti képpontokat jelenít meg a kijelzőn. Az érzékelő pixele, azaz képpontja, hőmérséklet érzékelőket tartalmaz. [41]

Az oktatási intézményekben számos olyan tanterem, valamint laboratórium található, ahol ajánlatos lehet hőérzékelős kamerákat elhelyezni. Ezek a következők:

- Szerverszoba,
- Raktárak,
- Különböző laboratóriumok,
- Számítógépes termek.

Adminisztratív tevékenységeket végző helyiségekben, ahol sok a számítógép és a papírmunka. Ilyen lehet az iskolai ügyintézők irodai.

A hőérzékelős kamerák minden esetben hasznosak. A fentebb felsorolt termekben a nap 24 órájában ritkán tartózkodnak, azonban a számítógép és az elektronikai berendezés meghibásodhat és tűz keletkezhet. Ilyen esetben az időbeni észlelés és riasztás kulcsfontosságú. A biztonsági hőérzékelős kamerák egy esetleges tüzet gond nélkül képesek nyomon követni, illetve a téves riasztások számát is csökkenthetik, mivel a kamera képének segítségével leellenőrizhető, hogy az adott helységben keletkezett-e tűz.

2 BLOKKLÁNC TEHNOLÓGIA

A kutatásomban a legnagyobb hangsúlyt a blokklánc alapú adattárolási megoldásokra fektettem, valamint azok specifikus jellemzőit vizsgáltam az ÓUDSC nevű egyetemi blokklánc létrehozása előtt. Vizsgáltam az ebben rejlő lehetőségeket, mivel a „hagyományos" felhő alapú tárhelyekről számos esetben kiderült, hogy nem nyújtanak kellő biztonságot. Külön aggodalomra adhat okot, ha érzékeny adatokat tárolásáról van szó. Az egyetemi hallgatói jelenléti ív, valamint a hallgatókról készült videófelvételek mindenképpen érzékeny adatoknak minősülnek, amelyek kompromittálódását meg kell előzni.

2.1 Mi a blokklánc?

A blokklánc számos blokkból tevődik össze, amelyet az adatbányászok hoznak létre. Ezek a blokkok időrendi, illetve adatbányászati sorrendben egymással összekapcsolódva egy láncot képeznek. Ezek fenntartása az adatbányászok feladata.

A blokkláncot nevezhetjük akár főkönyvnek is, ebben az esetben a lapok egy-egy blokkot jelentenek. A főkönyvek minden adatbányásznál megtalálhatóak, ezért az övék a megosztott felelősség is, így megkerülve az olyan szervezeteket, akik különböző adatvagyonok felett ellenőrzést gyakorolnak.

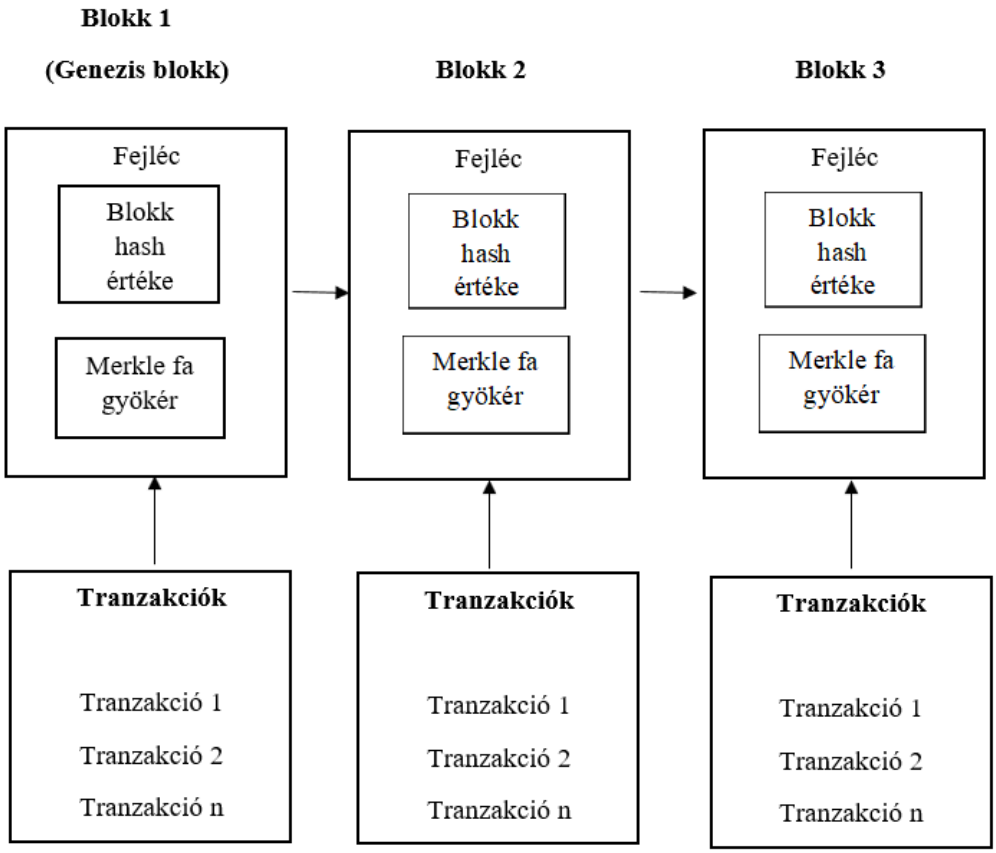
A nagymennyiségű adatok megjelenésével (Big Data) a hálózatok gyakran túlterhelté válnak. A blokkláncok a megosztottságukból kifolyólag lehetővé teszik a hatékonyabb adatfeldolgozást és költségcsökkentést. [42]

Számos informatikus és különböző szakember vélekedik úgy, hogy a blokklánc technológia lesz az új innovációs hullám. Meglátásaik szerint olyan technológiává fog válni, mint a gőzgép, az energiaellátás, az információ, valamint az internetes technológia. [43]
A blokklánc első blokkja a genezis blokk, erre épül a többi. Ezt követően minden blokk kapcsolódik az előző úgynevezett szülői blokkhoz. A blokk fejlécből és testből áll. A felépítésük a következő:

- Blokk verzió: a blokk érvényesítéséhez szükséges szabályokat tartalmazza,
- Szülői blokk hash kivonat: ez egy 256 bites érték, amely minden esetben az előző blokkra mutat. Ez nélkül a lánc nem jöhetne létre,
- Merkle fa gyökér kivonat: az összes blokk minden tranzakciójának a kivonatát képezi,

- Időbélyeg: aktuális időbélyeg másodpercenkénti lebontásban. Ez a hitelesítéshez szükséges,
- nBits: az aktuális hash érték kompakt formátumban kifejezve,
- Nonce: 4 bájtos mező, amely 0-val kezdődik és folyamatosan növekszik a hash számítások alkalmával. [44]

A második ábra a blokklánc struktúráját mutatja be.



2. ábra. Blokklánc struktúra [45]

2.2 A nyilvános és privát blokkláncok tulajdonságai

A nyilvános blokklánchoz bárki csatlakozhat és részt vehet annak működtetésében. Decentralizáltságának köszönhetően a döntéshozatalt és az érvényesítést külső behatástól függetlenül a Proof of Work, valamint a Proof of Stake mechanizmus hatja végre. Minden résztvevő működtetheti a csomópontokat, illetve adatbányászat útján a blokklánc tokenjét saját kapacitásától függően létrehozhatja. Az átláthatóság érdekében minden adat nyilvános. [46] Ez

azonban nem kedvez az érzékeny iskolai adatoknak, ezért a nyilvános blokklánc választása nem megfelelő.

A hálózaton belül bárki írhat, olvashat, és auditálhatja az aktuális tevékenységét. A csomópontok összegyűjtik a tranzakciókat, valamint ellenőrzik azok érvényességét és elindítanak egy konszenzusos protokollt a blokkok láncba történő kapcsolása céljából. Előfordulhat, hogy egyszerre két blokk is csatlakozni szeretne a blokklánchoz, ezért a blokk akkor tekinthető megerősítettnek, ha azt legalább 6 másik követi. [47]

A nyilvános blokklánc hátránya, hogy működése igencsak áramigényes. Ez tulajdonképpen a decentralizációból, illetve a nyilvános főkönyvből adódik. A szabályok betartásáért a hálózat minden tagja felel, mivel részt vesznek a tranzakciók hitelesítésében. Ez a művelet, illetve a blokklánc fenntartása hatalmas árammennyiséget igényel. A nyilvános blokkláncba, amit beírnak azt utólag megváltoztatni nem lehet, mivel a blokkok egymásra épülnek. [48]

A blokkláncban rögzítésre került adatok visszamenőleg nem módosíthatóak. [49] A nyilvános blokklánc felépítéséből adódóan érzékeny adatok tárolására nem alkalmas, mivel azokat bárki megtekintheti. Kijelenthető, hogy az oktatási intézmények esetében a hallgatókról készült videófelvételeket nem érdemes nyilvános blokkláncokban tárolni.
A privát blokkláncokat magánjellegű blokkláncoknak is szokták nevezni, mivel kizárólag azok használhatják, akik „meghívóval” rendelkeznek. A hálózati szabályok eltérhetnek, ugyanis ezeknek a szabályozását az alkotójuk határozza meg. A felhasználók a szabályozásba nem szólhatnak bele, azokat nem módosíthatják. Különösen érzékeny adatok esetében előnyös lehet ezt a megoldást választani. Külföldön az egészségügyben már használják a privát blokkláncot. [50]

Az egyetemi videófelvételek tárolása során javaslom a privát blokklánc használatát, mivel érzékeny adatokról van szó, amely a hallgatók személyes adatait tartalmazza. [51]
Ez esetben két lehetőség közül lehet választani:

- Már meglévő privát blokklánchoz való csatlakozás. Ezek a következő rendelkezésre álló kész megoldások lehetnek: FileCoin és az IPFS (Interplanetary File System – Peer - to - Peer alapon működő tartalomcentrikus blokktároló).
- Egyetemi privát blokklánc létrehozása saját szabályozás mellett.

A privát blokklánc a következő tulajdonságokkal rendelkezik:

- A blokklánchoz való csatlakozáshoz meghívóval kell rendelkezni. Ennek birtokában lehet kérelmezni a kapcsolódást, amelyet minden esetben azonosítás előz meg.
- A privát blokkláncokra jellemző, hogy emberi beavatkozást igényelnek (napi adminisztráció, hibaelhárítás, javítás).
- Minimális szintű központosítás szükséges, amely bizonyos mértékű centralizációhoz vezet. Ez az emberi beavatkozás szükségszerűségéből adódik. Ilyen lehet a jogosultságok kezelése, blokklánc karbantartása, működési szabályzat meghatározása. Fontos a megbízható csomópontok létrehozása. [52]

Azok a felhasználók, akik csatlakoznak a hálózathoz részt vesznek annak működtetésében és fenntartásában. [53]

Nem mellesleg a blokklánc használatért fizetni kell. A második táblázat a nyilvános és a privát blokklánc közötti különbségeket szemlélteti:

Blokklánc típusok		
Tulajdonságaik	Nyilvános	Privát
Hozzáférés	Bárki számára hozzáférhető	Kizárólag a meghívott felhasználók számára
Ki írhat a blokkáncba?	Akárki	Regisztrált, belépési engedéllyel rendelkező felhasználók
Felhasználók száma	Millió felhasználó	Néhány száz felhasználó
Biztonság	Proof of Work, Proof of Stake	Előre jóváhagyott résztvevők
Sebesség	Lassú (akár 10 perc is lehet a tranzakciós jóváhagyás)	Gyors (néhány másodperc alatt elegendő a jóváhagyáshoz)
Résztvevők	Névtelen	Ismert, azonosított

2. táblázat. Különböző blokklánc típusok tulajdonságai, (saját szerkesztéssel módosított) [54]

2.3 Okos szerződések

Az okos szerződés segítségével az NVR összekapcsolható a blokklánccal, valamint képes az adatok automatizált mentésére. Képes szabályozni a hozzáférési jogokat, ehhez mindössze a szerződési feltételeket kell meghatározni.

Az okos szerződés vagy más néven Smart Contract egy olyan blokklánc technológián alapuló megoldás, amely automatikusan hajtja végre a benne meghatározott feltételeket egy külső harmadik fél, mint végrehajtó személy megkerülése által. Ilyen esetben nincsen szükség ügyvédre a szerződés megkötésekor sem annak érvényesítésekor. Kizárólag olyan utasításokat hajt végre, amelyek a szerződési feltételekben előre meg lettek határozva. Ezeket a feltételeket triggereknek hívják. Az okos szerződés megkötésekor a következő 4 feltételre van szükség:

- Szerződés tárgyára, amelyről valójában szól a szerződés,
- Feltételek pontos meghatározására. Kizárólag azok teljesülése esetén lehet végrehajtani a szerződésben foglaltakat,
- Hitelesítésre. A digitális aláírással hitelesíteni kell a szerződés tárgyát, valamint annak feltételeit,
- Nem utolsó sorban pedig egy blokkláncra is szükség van, ahol létrejöhet a szerződés. [55]

Az okos szerződés tulajdonságai:

- Folyamatosan önmagát ellenőrzi,
- Önmagát futtatja a blokklánc csomópontjain, ezért elérhető a nap minden órájában. A felhasználóknak mindössze Internet csatlakozásra van hozzá szükségük.
- Manipulálhatatlan, mivel a kódot utólag módosítani nem lehet. A betáplált adatokat idegen nem tudja felülírni. [56]
- Az okos szerződés életútja nem módosítható, annak tartalma végrehajtásra kerül. [57]

Az okos szerződés előnyei a következők:

- Állandóság. A szerződésben meghatározott feltételek automatikusan végrehajtódnak, amennyiben azok teljesülnek.
- Átláthatóság. Az okos szerződésben rögzített feltételek a többi résztvevő számára nyilvános.

- Gyorsaság. Mivel nincsen szükség emberi beavatkozásra, így a szerződésben foglalt feltételek automatizáltan rövid időn belül végrehajtódnak. [58]

Az okos szerződés hátrányai:

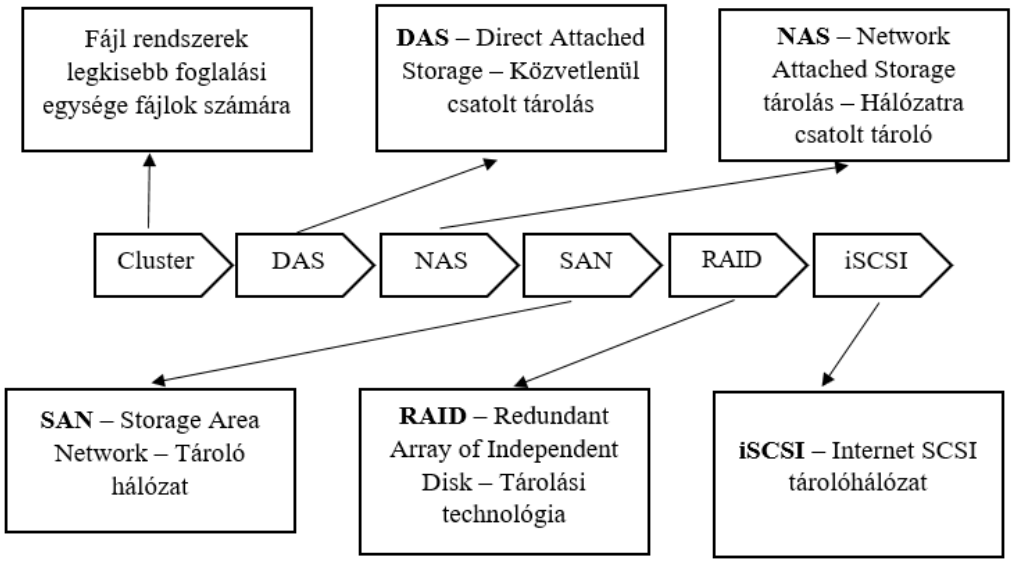
- Emberi hibák. Mivel az okos szerződés kódját emberek írják, ezért előfordulhatnak benne hibák. Amennyiben ezt a programozó nem veszi észre időben, úgy a hibás okos szerződés bekerülhet a blokkláncba, ahol olyan feladatot hajt végre, amely a feleknek nem megfelelő. A blokkláncban levő hibás okos szerződés kódját utólag nem lehet módosítani.
- Jogi problémák. Az okos szerződések jövőképe állami jogszabályozás hiányában bizonytalan. Nem tudni, hogy mi fog történni akkor, ha az állami szervek szabályozni kezdik a szerződéseket.
- Decentralizációs struktúrából adódó negatívum. Jogsérelem esetén nincsen olyan központi szerv, aki kárpótolhatná a felhasználót. [59]

3 ADATTÁROLÁSI MEGOLDÁSOK

A hallgatói jelenléti ívkészítő rendszer esetében az elsődleges adattárolás az NVR merevlemezén történik. Ez után kerül sor az adatok mentésére a blokkláncban. Az NVR számos videótárolási megoldást alkalmaz, ezeket áttekintettem a jelenléti ívkészítés aspektusából. Az NVR kiválasztásánál a videótárolási architektúrák fontos szempontot játszanak, mivel elsődlegesen itt tárolódnak el az adatok. Másodlagos, hosszútávú adattárolási lehetőségként áttekintettem a centralizált és decentralizált megoldásokat. azon belül is a már rendelkezésre álló kész blokklánc technológiákat. Amennyiben blokklánc alapú adattárolás mellett tesszük le a voksunkat, úgy két lehetőség áll a rendelkezésünkre. Az egyik megoldás az, ha bérlünk egy adattárolásra alkalmas kész blokkláncot a másik megoldás viszont az, hogy mi magunk hozunk létre egyet. Ebben az esetben még nagyobb adatbázisbiztonságot tudunk kialakítani, mivel kizárólagosan mi határozzuk meg a saját blokkláncunk irányelveit és nem egy harmadik fél feltételeit kell elfogadnunk.

3.1 Általános NVR videó tárolási architektúrák

Az NVR egységek által alkalmazott fontosabb adattárolási architektúrák a harmadik ábrán tekinthetőek meg.



3. ábra. Tároló architektúrák [60]

A tárolási architektúrák fontos szerepet játszanak a videó fájlok rögzítésében, mivel ezek nagy mértékben kihatnak a videófelvételek biztonságos tárolására.

- DAS – Direct Attached Storage, a megosztott adatok tárolásának klasszikus módja a szerveren elhelyezett merevlemezek használata által. Nagyon sokáig használták ezt a megoldást. Hátránya, hogy amennyiben a szerverek leállnak, úgy a tárolók is elérhetetlenné vállnak. Nem utolsó sorban a DAS rendszer üzemeltetése tetemes költséggel jár. Ilyen lehet a jogosultságkezelés, partícionálás, illetve egyéb adminisztrációs kiadások. Ez nem egy esetben elérheti a beszerzésre fordított összeg 40 százalékát. [61]
- NAS – Network Attached Storage, egy fájl szintű adattároló eszköz, amely a számítógépes hálózathoz csatlakoztatva biztosítja az adatok megfelelő menedzselését a felhasználók között, legyenek azok akár egy másik földrészen is. Ezen felül internetkapcsolat segítségével bárhonnan elérhetőek. A tárolt adatok megoszthatóak, védhetőek a felhasználói engedélyek megfelelő beállításával. [62] A NAS saját operációs rendszerrel ellátott cél hardver, amely stabil működést tesz lehetővé. Számos platformról elérhető, úgy Linux, mint Windows alapú számítógépekről, illetve mobileszközökről. Leggyakrabban két NAS modellt különböztetnek meg, ezek az átlagfelhasználói, illetve üzleti modellek. [63]
- NAS előnyei:
  - Szabványos Ethernet és IP protokoll használata,
  - Kiterjedése korlátlan,
  - Fájlkezelés optimális teljesítménnyel,
  - A DAS-hoz képest sokkal jobban méretezhető.
- NAS hátrányai:
  - LAN túlterhelés/torlódás előfordulhat,
  - Általában speciális operációs rendszert alkalmaz,
  - A központosított fájlkezelés nem felel meg bizonyos blokk szintű hozzáférést igénylő alkalmazásoknak. [64]
- SAN – Storage Area Network, alrendszerekből és kapcsolókból áll. A merevlemezeket tartalmazó eszközök valamilyen gyors kapcsolaton keresztül egyfajta hálózatba vannak szervezve. Ez az alhálózat pedig a kapcsolókon keresztül elérhető a szerverek számára. A SAN jellemzően FibreChannel (FC) vagy IP felett elterjedő iSCSI protokollt használja. [65]

- RAID – Redundant Array of Independent Disk, egy olyan megtöbbszörözött tárolóegységet jelent, amelyet a rendszer és a felhasználó egyetlen tárnak lát. Minimum két darab merevlemezt használ. A RAID nem egy konkrét módszer – több alfaja is ismert. Az NVR-ek többsége támogatja a RAID megoldásokat. Ezek a következők: RAID 0, RAID 1, RAID 5 és a RAID 10. [66]
- RAID 0 gyors működést tesz lehetővé, mivel a tárolóegységek úgy vannak összekapcsolva, hogy az adatblokkokat különböző, egymás utáni merevlemezekre menti el.
- RAID 1 esetében az adatok párhuzamosan kerülnek mentésre. Egyszerre két merevlemezre kerül ugyanaz az adat. Ajánlatos, hogy a merevlemezek nagysága megegyezzen, mivel a RAID 1 a kisebb merevlemez nagyságot veszi figyelembe, amennyiben azok eltérnének egymástól.
- RAID 5 kiépítéséhez legalább 3 meghajtó szükséges. Támogatja a hardver alapú paritást. Amennyiben egy merevlemez megsérül, adatvesztésre nem kerül sor. A legtöbb NVR ezt a megoldást alkalmazza.
- RAID 10 kialakításához legalább 4 merevlemezre van szükség, melyeket előbb RAID 1-ben tükrözik párosával, majd ezeket a tömböket csíkozzák. A megoldás előnye, hogy megadja az adatbiztonságot és a sebességet is, viszont a tárhely a RAID 1-nél megismert tükrözés miatt feleződik. [67]
- iSCSI - Internet Small Computer Systems Interface, egy IP-alapú hálózati kommunikációs szabvány adattárak (storage-ok) összeköttetésére szolgál. A kliens (initiator) SCSI parancsokat (CDB) küld IP-hálózaton keresztül a SCSI storage-nak (targetnek). A CDB (Command Descriptor Block) a kliens által küldött parancs, mely tartalmazza a Logical Unit Number-t (LUN), a logikai egység számát. Ez jelöli a külön címezhető logikai SCSI eszközt, amely a target-nek (fizikai SCSI eszköznek) a része [68].

A fentebb felsorolt NVR adattárolási megoldások közül a RAID 5, illetve a RAID 10 a lehető legjobb választás a jelenléti ívkészítő rendszer számára, mivel ugyanazokat az adatokat több merevlemezen is eltárolja. Amennyiben az egyik merevlemez megsérülne, illetve vírusos támadás áldozatává válna, úgy a többi merevlemez használata által az adatok az eredeti állapotukban helyreállíthatóak maradnának.

3.2 Adattárolási megoldások típusai

A fizikai eszközökön történő adattárolás mindenki számára jól ismert. A közelmúltban a felhőben tárolt adatok új távlatokat nyitottak meg. Az online jelentléti ívkészítő rendszer tervezése során megvizsgáltam ezeket a lehetőségeket. A felhőalapú megoldások már bizonyították előnyüket a könnyű hozzáférés és szinkronizáció által, amelyek megkönnyítik az adatok rögzítését.

Az adatok tárolása a gyakorlatban a következőképpen néz ki:

- Fizikai eszközökön történő mentés. Ilyen lehet az NVR merevlemeze, valamint a pendrive és a különböző lemezek (CD, DVD, Blue-Ray),
- Centralizált felhőben történő adattárolás. Az adatok a felhőben kerülnek tárolásra, amelynek külön tulajdonosa és üzemeltetője van. A szerver üzemben tartója felel az adatok biztonságáért.
- Decentralizált felhőalapú adattárolás esetében az adatokat decentralizált hálózaton tárolódnak. Az adatok mentése nem egy vállalat szerverén történik, hanem olyan számítógépeken, amelyeket egymástól független egyének üzemeltetnek a világ számos pontján. Az okos szerződések által lehet csatlakozni az ilyen hálózatokhoz.

A centralizált felhőalapú adattárolás esetében számos olyan nem kívánatos esemény történt a múltban, amely aggodalomra adhat okot. Az adatszivárgás nem egy esetben előfordult. A jelenléti ívkészítő rendszer esetében a cél a lehető legnagyobb biztonság elérése, ezért megvizsgáltam a rendelkezésre álló adattárolási lehetőségeket, illetve olyan új megoldások után kutattam, amelyek a lehető leghatékonyabb biztonságot képesek nyújtani.

A felhő alapú adattárolás esetében az alapfeltételezés az, hogy a harmadik fél egy megbízható szolgáltató, akinek a célja, hogy az adatok mindvégig biztonságban legyenek és a nap 24 órájában rendelkezésre álljanak. Előfordulhat, hogy a harmadik fél károsítja az adatokat a saját személyes javára. Módosíthatja, kiadhatja különböző szerveknek, illetve törölheti is azokat. Ennek kivédése érdekében több felhőalapú tárolási platformot szoktak egyszerre használni. Hátránya, hogy ez a módszer nagy hálózati forgalmat és sávszélességet generál. [69]

Az adatok a harmadik féltől való megóvása érdekében ajánlatos titkosítani és úgy feltölteni a felhőbe. A centralizált tárolórendszerek a következő gyengeségekkel rendelkeznek:

- Biztonság. Amennyiben illetéktelen személy hozzáfér a szerver adataihoz, úgy azok kompromittálódhatnak.
- Megbízhatóság. A szerver túlterhelté válhat, ha egyszerre túl sok lekérdezés érkezik. A DDoS (Distributed Denial of Service Attack - Szolgáltatásmegtagadással járó támadás) támadások így működnek.
- Adatátviteli sebesség. A szerverrel való gyors kapcsolat szükségszerű. Ha a felhasználók számítógépei különböző országokban vannak (általában ez a jellemző), akkor az adatátviteli sebesség csökkenhet, illetve egyes országok korlátozásokat is kiszabhatnak.
- Skálázhatóság. A központosított kialakítás következtében a szerver kapacitása korlátozott, valamint az adatforgalom is szabályozott. [70]

Megállapítottam, hogy a centralizált adattárolási megoldásnak számos gyenge pontja és hiányossága van, ezért annak alkalmazását a jelenléti ívkészítő rendszer esetében elvetettem.

A decentralizált adattárolási megoldásnak köszönhetően az adatok nagyobb biztonságban vannak, mint a felhő alapú tárolás esetében, hiszen azok elosztva számos csomóponton helyezkednek el. Továbbá a tárolórendszerek nyilvános kulcsú titkosítást használnak. Az adatokat a csomópontok között rugalmasan osztják szét, valamint okos szerződéseket is alkalmaznak az automatikus végrehajtás céljából. [71]

A Decentralizált adattárolás előnyei:

- A teljesítmény kiegyensúlyozott, mivel a csomópontok arányosan osztoznak az adatmennyiségeken,
- Magas rendelkezésre állás. A csomópontok többsége rendelkezésre áll a nap 24 órájában. Amennyiben egyes csomópontok (node) elérhetetlenné vállnak, úgy a többi továbbra is kiszolgálja a felhasználót.
- Magas fokú önállóság. Minden csomópont önállóan felel a szabályok betartásáért, így alakítva ki a blokkláncot ökoszisztémát. Kívülálló személy, illetve hatóság nem korlátozza, illetve szabályozza a működését.
- A felhasználók adatait feldarabolja, majd pedig titkosítva küldi szét a csomópontoknak. DDoS támadás esetén a rendszer működőképes marad.

- Ha egyes csomópontok nem működnek, illetve elérhetetlenné vállnak támadás esetén a többi csomópont zavartalanul működhet tovább. A centralizált rendszerben, ha a központi szerver leáll, akkor nagy valószínűséggel az egész rendszer működésképtelen lesz, ezért az adatokhoz nem lehet hozzáférni. [72]

Hátrányai:

- A központi felügyelet hiányából adódóan, nincsen parancslánc, amely parancsokat adhatna különböző feladatok elvégzésére.
- Hiányzik az úgynevezett „megszokott" szabályozási felügyelet. A privát blokklánc létrehozója meghatározza a szabályokat, amelyek az okos szerződés keretében kerülnek betartásra. Ez néhány esetben nehezen átlátható.
- Körülményes meghatározni, hogy melyik csomópont sikertelen, mivel minden egyes csomópontot le kell ellenőrizni.
- Nehéz megállapítani, hogy melyik csomópont válaszolt a kérésre, mivel decentralizált rendszer révén több csomóponton is rendelkezésre állnak ugyanazok az adatok. [73]

Megállapítottam, hogy a decentralizált adattárolás esetében az adatok számos csomóponton egymástól teljesen függetlenül tárolódnak, amely biztonságnövelő tényező, ezért ez a típusú blokklánc technológia alkalmas arra, hogy hosszútávon a jelenléti ívkészítő rendszer részét képezze. Ennek függvényében további kutatásokat végeztem. Részleteiben vizsgáltam az On-Chain és Off-Chain blokklánc technológiát.

3.3 On-Chain és Off-Chain adattárolás

A decentralizált blokklánc alapú adattárolásnak két jelentősebb megvalósítása létezik. Ez az On-Chain és Off-Chain blokkláncok.

Az On-Chain a legbiztonságosabb blokklánc alapú adattárolási megoldás, mivel minden adat minden blokkban mentésre kerül. Ennek következtében a hálózat működése lelassulhat, extrém esetben elérhetetlenné is válhat a túlterhelés miatt. Ezen felül a csomópontok megőrzik az összes adatot, folyamatosan szinkronizálódnak egymással. Amennyiben támadás történik az adatok nem vesznek el. Ez egy drága, de biztonságos megoldás. [74]

A nagyobb felbontású videófelvételek tárolása, mint amilyen a:

- HD,
- Full HD,
- Valamint a 4K felbontás komoly adatmennyiséget generálnak.

Ezeket az adatokat blokkonként elmenteni nem érdemes, mivel az On-Chain a kisebb adatok, illetve szöveges fájlok tárolására lett kitalálva, ezért az oktatási intézményeknek ezt a megoldást nem érdemes választaniuk. Helyette ajánlatos az Off-Chain tároláson elgondolkodniuk.

Általában a blokkláncok különböző tranzakciókkal kapcsolatos információkat tárolnak, ezért kis blokkmérettel rendelkeznek. Ezt részletesen a negyedik táblázat szemlélteti:

Coin megnevezése	**Blokkok mérete**	**Blokklánc mérete**	**Napi új blokkok száma**
Ethereum Classic	1,3 KB	3.8 GB	6695
Ethereum	30KB	132 GB	2232
Dash	2MB	23GB	244
DigiByte	0.5KB	1,9MB	1152

3. táblázat. Különböző érme típusok blokklánc méretei [75]

Az Off-Chain nem tárol el minden egyes adatot csomópontonként, helyette azok hash értékét rögzíti. Az adatok tényleges tárolása az adatbányászok merevlemezén történik. Ezeket az adatokat mentés előtt több példányban feldarabolják. Az adatbányászok coin-okat (digitális érméket) kapnak a szolgáltatásaikért. [76]
A hash nagyban hasonlít az adat ujjnyomatára és algoritmusára, amely a különböző adatokból ujjnyomatot csinál az SHA-256 (Secure Hash Algorithm - Kriptográfiai Hash függvény) függvény segítségével. A blokkmódosítást, illetve hash módosítást minden bányásznak el kell fogadnia és hitelesítenie kell, hogy az érvényes maradjon. [77]

Megállapítottam, hogy a decentralizált Off-Chain technológia nyújtja a leghatékonyabb és egyben a legbiztonságosabb adattárolási megoldást a jelenléti ívkészítő rendszer számára, ezért következő lépésként a gyakorlatban is rendelkezésre álló Off-Chain adattárolási megoldásokat vizsgáltam.

3.4 Blokklánc alapú adattárolási megoldások napjainkban

Nagyobb adatmennyiségek tárolása érdekében különböző blokklánc alapú megoldások jelentek meg az utóbbi években. Mint minden újdonság ez is gyerekcipőben jár. Mivel komoly lehetőségek rejlenek bennük, ezért érdemes velük behatóbban foglalkozni. Ha a felvételek tárolása az elsődleges cél, úgy az alábbi kész blokklánc megoldások közül lehet választani:

- IPFS,
- FileCoin.

Az online jelenléti ívkészítő rendszer esetében szükséges megvizsgálnom, hogy a már fentebb említett kész blokklánc megoldások alkalmazása lenne-e a jobb választás, illetve egy saját egyetemi blokklánc létrehozása, amelyet az oktatási intézmény felügyel. A kész blokklánc megoldásnak az előnye, hogy nem kell a létrehozásával bajlódni, valamint bonyolult konfigurálási megoldásokkal sem szükséges foglalkozni. Ebben az esetben, ahogy az előfizetés megtörténik, úgy a blokklánc rögtön a rendelkezésre áll.

A FileCoin lehetővé teszi, hogy központi szerver nélkül lehessen adatokat tárolni. Az adatfájlokat a nagyobb szolgáltatók, úgy, mint a Google Drive, Dropbox megkerülése által is lehetséges tárolni, ehhez Peer-to-Peer hálózatra van szükség. Ilyen esetben a felhasználók nem a szerverszolgáltatóknak fizetnek, hanem a FileCoin hálózat adatbányászainak, akik önkéntes szabad tárhellyel rendelkeznek. A tárhelyért cserébe coin-t (érmét) kapnak, amely szabadon eladható, vagy készpénzre cserélhető. A FileCoin ugyanúgy, mint a többi decentralizált szolgáltatásnak a következő hátrányai vannak:

- Magas volatilitás, ezért jelentős bizonytalanság övezi,
- Nehezen skálázható,
- Számos esetben lassabbak, mint a centralizált társaik. A sebesség igencsak adatbányászfüggő. Minél több adatbányász kapcsolódik a blokklánchoz az annál hatékonyabbá válik. [78]

Az IPFS célja, hogy az összes számítógépes rendszert összekapcsolja ugyanazzal a fájlrendszerrel. Ez is Peer-to-Peer alapon működik. Előnye, hogy nincs központi szerver, valamint, hogy az adatokat a világ különböző helyein tárolja.

A többi rendszerhez képest nagy teljesítményű blokktárolási modellt kínál, amelyben tartalom és címzett hivatkozások találhatóak. Továbbá a DHT (Distributed Hash Tables - Elosztott Hash táblák) megoldásokat egyesíti az önhitelesítő névterekkel.

Előnye, hogy az IPFS csomópontoknak nem szükséges megbízniuk egymásban, így csökkentve a meghibásodás lehetőségét. Egyetlen hátránya, hogy nem nyújt erős adatvédelmi és kriptográfiai megoldást. [79]

Az IPFS mivel blokkokból épül fel, ezért az adatok tárolására a már rendelkezésre álló blokkokat használja fel. Ezen felül link táblázatot is tartalmaz, amely további blokkokra mutat rá. Minden blokkhoz tartozik egy hash érték, ez alapján lehet őket elérni. A felesleges adatmásolatok elkerülése érdekében az összes változat ugyanarra az adatcsomagra mutat, így a hash segítségével az adatok átfedése kiszűrhető. Ezzel a módszerrel értékes tárhelyet lehet megtakarítani. A rendszer lényege, hogy a fájlok egy példányban tárolódnak el, ezért a blokkok egyszer képződnek le. A biztonság növelése érdekében egy blokkot többen is tárolhatnak, ez által az elérhetőség is arányosan növekszik. [80]

Az IPFS esetében az okos szerződés használatára is adott a lehetőség. Az adatot első lépésként az IPFS-ben kell feltölteni, ahol az adat kivonatának generálása után az visszakerül a tulajdonosához. Az okos szerződés feladata az adatbányászok lekérdezése és azonosítása. Ezt követően a kulcspárok tárolása történik és a titkosítás megosztása az arra jogosult személy számára. A tárolt adatokhoz való hozzáférésért természetesen fizetni kell. Ennek végrehajtása az okos szerződés feladata. Ez követően az adatbányászok visszakeresik a titkosított kivonatot, így a vevő le tudja tölteni az adatokat. [81]

Miután áttekintettem az IPFS és a Filecoin adattárolási megoldásokat, arra a következtetésre jutottam, hogy az elérhető legnagyobb adatbázis biztonság érdekében egy saját egyetemi blokkláncot hozok létre, ahol személyesen tudom szabályozni az adatokhoz való hozzáférési jogosultságokat.

4 ADATBÁZIS-BIZTONSÁG

Az adatbázis-biztonsághoz kiemelt fontosságú a személyazonosításra alkalmas jelenléti ívkészítő rendszer esetében, ezért megvizsgáltam a lehetséges iskolai adatbázisokat fenyegető veszélyeket. Mivel a jelenléti ívkészítő rendszer videófelvételeket is képes rögzíteni, ezért áttekintettem a magyarországi a szerbiai és az Európai Unió elektronikus megfigyelőrendszereire vonatkozó adattárolási törvényeket. Célom, hogy az adatok az aktuális jogszabályoknak megfelelően biztonságosan kerüljenek rögzítésre.

4.1 Lehetséges iskolai adatbázisokat fenyegető veszélyek

A jövőben az adatbázis-biztonság még inkább előtérbe fog kerülni, mivel az adatmennyiségek egyre inkább növekednek. Jelenleg az 5G hálózat kiépítése zajlik, amely új távlatokat nyithat meg a kommunikációban. Könnyen belátható, hogy megfelelő adatbázisbiztonság nélkül az 5G-s megoldások veszélybe kerülhetnek.

Az iskolai adatok mennyisége folyamatosan növekszik. A digitalizáció korában a papírlapú dokumentumok jelentősen lecsökkentek, helyettük a digitálisan rögzített adatok vették át a szerepet. Előnyük, hogy adatbázisban rendezve könnyen áttekinthetőek, gyorsabban hozzáférhetőek. Hátrányuk a nagyobb sebezhetőség, mivel ezek az adatok rendszerezve, strukturálva kerülnek rögzítésre, így egy adatbázis feltörése esetén a támadó könnyen átláthatja az illetéktelenül megszerzett információkat. [82]

Az oktatási intézményeknek fel kell készülniük ezekre a veszélyekre. Nem csak a kamerafelvételek biztonságos tárolása fontos, hanem a hallgatók azon személyes adatai is, amelyekkel az egyetemek rendelkeznek. A modern e-Learning megoldásoknak köszönhetően a tananyagokat már nem csak prezentáció formájában lehet elkészíteni, hanem a videófelvételek által azokat színesebbé is lehet tenni. Fontos szempont kell, hogy legyen az oktatási intézmény és a hallgatók közötti biztonságos és gyors Internetkapcsolat kialakítása. A jövőben az oktatási intézményeket a következő új típusú veszélyek fenyegethetik:

- A kártékony programok azonosítása nehezebbé válhat, mivel azok megtanulják utánozni a rendeltetésszerű felhasználói viselkedést. Ez által azok nehezebben lesznek felismerhetőek.

- A hagyományos felhőalapú centralizált megoldások növelhetik az esetleges sikeres támadások kockázatát, mivel azok gyenge pontjait ez idáig a támadók sikeresen kiismerhették.
- Megjelenhetnek az automatizált támadási megoldások a mesterséges intelligencia alkalmazása által. Ezeket az intelligens támadásokat feltételezhetően nehezebb lesz majd kivédeni. [83]

Az oktatási intézmények a jövőben nem csak a videófelvételeket és ahhoz kapcsolódó metaadatokat tárolhatnák a blokkláncban, hanem akár tananyagot is. A privát blokklánc által szabályozni lehet a hallgatói hozzáféréseket különböző jogosultságok függvényében. Az egyetem a blokklánc csomópontjaira feltöltheti az oktatáshoz szükséges leckekönyvet, amelyet a hallgatók a saját okos eszközeikre letölthetnek. Ez által a hallgató és az oktatási intézmény között egy teljesen új biztonságos kapcsolat jön létre.

4.2 Számítógépes bűncselekményekre vonatkozó adattörvények

A számítógépes bűncselekmények meghatározása már a 2001-es számítógépes bűnözésről szóló Egyezmény (Convention on Cybercrime) aláírásakor megjelent, ugyanakkor Magyarország ezt csak jóval később, 2004-ben hirdette ki, [84] illetve tett eleget az Egyezményben vállalt, a magyar jogrendbe való beemelési (implementálási) kötelezettségnek. A BTK (Büntető Törvénykönyv) XLIII. fejezetben a következő cím alatt található: „Tiltott adatszerzés és az információs rendszer elleni bűncselekmények”. A fejezet különálló törvényi tényállások szerint szabályozza az információs rendszereket közvetlenül érintő elkövetési magatartásokat.
A 422.§ törvényi szabályozásában tiltott adatszerzésre lett változtatva a magántitok jogosulatlan megismerése, így az bűncselekménynek minősül.

A 2001-es Egyezmény alapján fogalmazták meg az információs rendszerben tárolt adatok megőrzésre kötelezésének és az elektronikus adat ideiglenes hozzáférhetetlenné tételének, mint kényszerintézkedéseknek, az új eljárásjogi szabályait. Ennek az intézkedéseknek az elsődleges célja, hogy a tárolt adatok és információk a büntetőeljárás elejétől egészen a bírósági szakasz végéig felhasználhatóak legyenek bármikor. Az illegális tartalmakat blokkolják úgy, hogy azok ne vesszenek el, illetve semmisüljenek meg, azok bizonyító erejűek maradjanak. Ezek végrehajtásában, illetve kényszerintézkedések alkalmazása által határozott segítséget nyújt a belügyminisztérium irányítása. [85]

Az oktatási intézményeknek a videófelvételek tárolásáról szóló szabályzatokat ismerniük kell. Előfordulhat, hogy a biztonság érdekében rögzített képeket rossz indulatú támadók illegális célokra felhasználják, ezért a biztonsági felvételeket szigorúan szabályozzák. [86]
A GDPR (General Data Protection Regulation - Általános adatvédelmi rendelet) esetében a következő szabályokkal, illetve alapfogalmakkal ajánlatos tisztában lenni:

- A GDPR rendelet értelmében személyes adatnak minősül minden olyan adat, amely alkalmas a természetes személy azonosítására.
- Adatkezelés alatt a személyes adatokkal való műveletek értendőek, ezért azokkal megfelelően, jogszerűen kell eljárni.
- Adatgyűjtés során fontos, hogy az adatok biztonságban legyenek, valamint az adatkezelési szabályok szigorúan be legyenek tartva.
- Adatkezelőnek tekinthető az a személy, aki megszabja az adatkezelés célját, továbbá azzal kapcsolatos döntéseket hozhat.
- A meghatározás szerint adatfeldolgozó az a személy, aki más nevében használ személyes adatokat. [87]

Az EU 2016. április 6.-án megállapodott az adatvédelmi keretének átalakításáról, jóváhagyva a húszéves 95/46/EK irányelv és rendőrségi irányelv helyébe lépő általános adatvédelmi határozatot (GDPR) tartalmazó adatvédelmi módosítási csomagot, melynek rendelkezései 2018. május 25. óta használhatóak. A magyarországi adatvédelemmel kapcsolatos környezet GDPR egyenértékű keretében egyrészt 2018. augusztus 25-i hatállyal megtörtént az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény legelső módosítása. 2019. április 26.-án pedig nyilvánosan is megjelent. [88]

A biztonsági felvételek megfelelő tárolása érdekében ez idáig előre meghatározott időtartam volt kiszabva. A rögzített felvételeket három munkanap után törölni kellett. A működtetett rendszerek többsége önállóan végrehajtva törölte a felvételeket meghatározott időn belül. Ez azonban problémát okozott, mivel a rendszer számára körülményes volt a folyamatosan változó munkanapok definiálása. Továbbá az adatkezelő részéről is rendszeresen felmerültek olyan egyedi helyzetek, amelyek a hosszabb megőrzési idő mellett érveltek. Mindezek a korlátok megszűntek. Az új szabályozásnak köszönhetően az adatkezelők akkor is szabályszerűen járnak el, ha egyéni igény szerint meghosszabbítják a már korábban pontosan meghatározott időintervallumot.

A szabályok módosítása előtt a kamerával megfigyelt területre belépő személy a belépéssel elfogadta, hogy róla felvételt készítenek és hozzájárult az adatkezeléshez. Azokban az esetekben, amikor nem egyezett bele, úgy az adatkezelés nem volt jogszerű. Az új uniós szabályok határozottan kizárják a ráutaló magatartással való hozzájárulást. A törvény módosítása után az adatkezelők részére egy teljesen új helyzet állt elő: akkor járnak el helyesen, ha a személy- és vagyonvédelmi célú megfigyelés jogalapjaként mindenképpen a jogos érdekeket jelölik meg. Ilyen esetben nem szükséges a hozzájárulás, kell viszont egy olyan érdekmérlegelési teszt, amely valamennyi kamerára kiterjedően alátámasztja azt az adatkezelői jogos érdeket, amely alapján lehetőség van az adatkezelésre. [89]

Megszüntetésre kerültek a rögzített felvételekhez köthető szigorú szabályozások, ebből kifolyólag a jövőben nem szükséges jogos érdekét igazolnia annak, aki a rögzített felvételbe betekintést kér. A szabály megjelenése után a kamerafelvételeket nem csak a bírósági, hanem a különböző hatósági eljárások során is szükségszerűen fel lehet használni. A törvény legnagyobb újdonsága, hogy jegyzőkönyvként is elismeri az elektronikus nyilvántartást. [90]

Szerbiában a videókamerák felvételeinek kezelését a személyes adatok védelméről szóló törvény szabályozza. Ez a Hivatalos Szerbiai Közlöny PC 97/2008 számában jelent meg, amely a Korrupció Elleni Ügynökség 15-ös számú törvényén alapszik. A törvény kimondja, hogy 30 napnál tovább a felvételeket nem lehet megőrizni. Kivételes eset az, amikor az a büntető, vagy vétség eljárás részét képezi.

A törvény kötelezővé teszi, hogy az objektumok bejárata előtt, illetve a beltéri területeken fel kell tüntetni a figyelmeztetést, miszerint az objektum videómegfigyelés alatt áll. Ezen felül minden emeletre ki kell azt helyezni, mint ahogyan a liftek ajtaja elé is. A videómegfigyelő rendszert úgy kell kiépíteni, hogy illetéktelen személy annak irányításához ne férjen hozzá. A megfigyelőrendszer telepítést kizárólag az engedéllyel rendelkező szakember végezheti el. A rendszer javításának feladata úgyszintén az ő feladatköre. Ilyen engedélyt kizárólag a MUP (Ministarstvo Unutrašnjuih Poslova – Belügyminisztérium) állíthat ki. [91]

Továbbá a munkáltatónak csak akkor van joga rögzíteni az alkalmazottak beszélgetéseit, ha azt a munkaköri leírásuk tartalmazza. [92]

4.3 Egyetemi Neptun, illetve elektronikus napló rendszer

A jelenléti ívkészítő rendszer esetében az elsődleges cél, hogy az elkészített jelenléti ívet az oktatók időben megkapják. Magyarországon ez történhet akár a Neptun rendszeren keresztül is. Szerbiában nincsen ilyen rendszer, helyette elektronikus naplót használnak az oktatási intézményekben. Az elektronikus napló leginkább az általános és középiskolákban elterjedt.

A Neptun egy Egységes Tanulmányi Rendszert jelent, amely számos online iskolai adminisztrációs tevékenység ellátásra szolgál. A Neptunon belül két fontosabb modult különböztetünk meg, úgy mint:

- Hallgatói modul,
- Tanári modul.

Ezek a modulok az Interneten keresztül érhetőek el. Az alkalmazásuk által könnyen elvégezhetőek az alábbi feladatok:

- Tárgyfelvétel,
- Vizsgákra jelentkezés,
- Hallgatók tájékoztatása emailen keresztül. [74]

Szerbiában jelenleg kevés egyetem használja az elektronikus naplót. A szerbiai helyzetet jellemzi, hogy az adminisztrációs feladatokat leginkább személyesen az oktatási intézményekben lehet elintézni. A gyakorlatban ez úgy néz ki, hogy az egyetemen az illetékesek beviszik a kívánt adatokat.

A gyakorlati megvalósítás során, ezért a jelenléti ívkészítő kamerarendszer a hallgatói hiányzásokat a tanároknak küldte el. A pedagógusok az email címükre kapták meg a hallgatói jelenléti ívet.

5 AUTOMATIZÁLT ELEKTRONIKUS BLOKKLÁNC ALAPÚ HALLGATÓI JELENLÉTI ÍV LÉTREHOZÁSA A GYAKORLATBAN

A személyazonosításra alkalmas automatizált elektronikus blokklánc alapú hallgatói jelenléti ívkészítő rendszert a gyakorlatban megvalósítottam. Létrehoztam az ÓUDSC egyetemi blokkláncot. Ezt követően meghatároztam az okos szerződés feltételeit, amelyet a jelenléti ívkészítő rendszer használ.

5.1 ÓUDSC (Óbudai University Data Storage Chain)

Az iskolai biztonsági kamerafelvételek tárolása érdekében egy saját privát blokklánc adatbázist hoztam létre, mivel ennek szükségességét a kutatásomban megállapítottam. A létrehozott blokklánc neve ÓUDSC, amely az Óbudai University Data Storage Chain rövidítést jelenti. Ez sokkal bonyolultabb feladat, mint bérelni egy mások által létrehozott decentralizált tárhelyet. Amennyiben az oktatási intézmény a bérlés mellett teszi le a voksát, úgy annak el kell fogadnia a szolgáltató által megszabott feltételeket. Az önálló egyetemi blokklánc esetében, az oktatási intézmény saját maga határozza meg a számára előnyős tárolási feltételeket. Ezek a következőek:

- Az oktatási intézmény szélesebb körű hozzáférést szerez a blokklánchoz,
- Blokkok nagyságát meghatározhatja,
- A felhasználási feltételeket definiálhatja,
- A genezis-legelső blokk, amelyhez az összes többi blokk csatlakozni fog az oktatási intézmény tulajdonában marad,
- Blokklánc hozzáférését korlátozhatja (csak az erre jogosultak használhatják azt),
- Az adatvédelmi politikát meghatározhatja,
- A blokkláncot több szerveren is el tudja indítani a biztonság érdekében,
- A csomópontokat könnyebben felügyelheti,
- Az oktatási intézmény számára a rendszer átláthatóbbá válik,
- Az okos szerződéseben foglalt feltételeket elsődlegesen ő saját maga határozza meg. [93]

A gyakorlati megvalósítás részeként létrehoztam az ÓUDSC nevű blokkláncot. Az alábbi ábra ezt mutatja be:

Egyetemi blokklánc létrehozása ÓUDSC néven

Az alapértelmezett blokklánc beállítások a következők voltak:

/default ~ universitychain/ÓUDSC/chainsettings.dat

chainsettings.dat a következő beállításokat tartalmazza:

Adatbázis címe [fogadó fél (a felhő tároló) IP címe, küldő fél (egyetem) IP címe],

Biztonsági kamerarendszer címe [fogadó fél IP címe, küldő fél (NVR) IP címe],

A GDPR adatbázis szabályzata. – A törvényi előírásnak való megfelelés.

Következő lépésként az ÓUDSC blokklánc kezdőértékét adtam meg, valamint a genezis blokkot is létrehoztam:

universitychain ÓUDSC

A blokk nagyságát definiáltam. A blokklánc gyorsasága érdekében 1 MB értéket adtam meg.

create block size: max limit 1MB/block.

Miután létrehoztam a genezis blokkot, elindítottam a szervert. A csomópont csatlakoztatási címe a következő volt:

universitychain ~ server 1

Az adatbázisbiztonság növelése céljából egy második szervert is elindítottam:

universitychain ~ server 2 ÓUDSC@192.168.0.2:8008

A biztonságos kapcsolat kialakítása után a blokklánc megvizsgálta a második szervert is, valamint a protokollokat is le ellenőrizte.

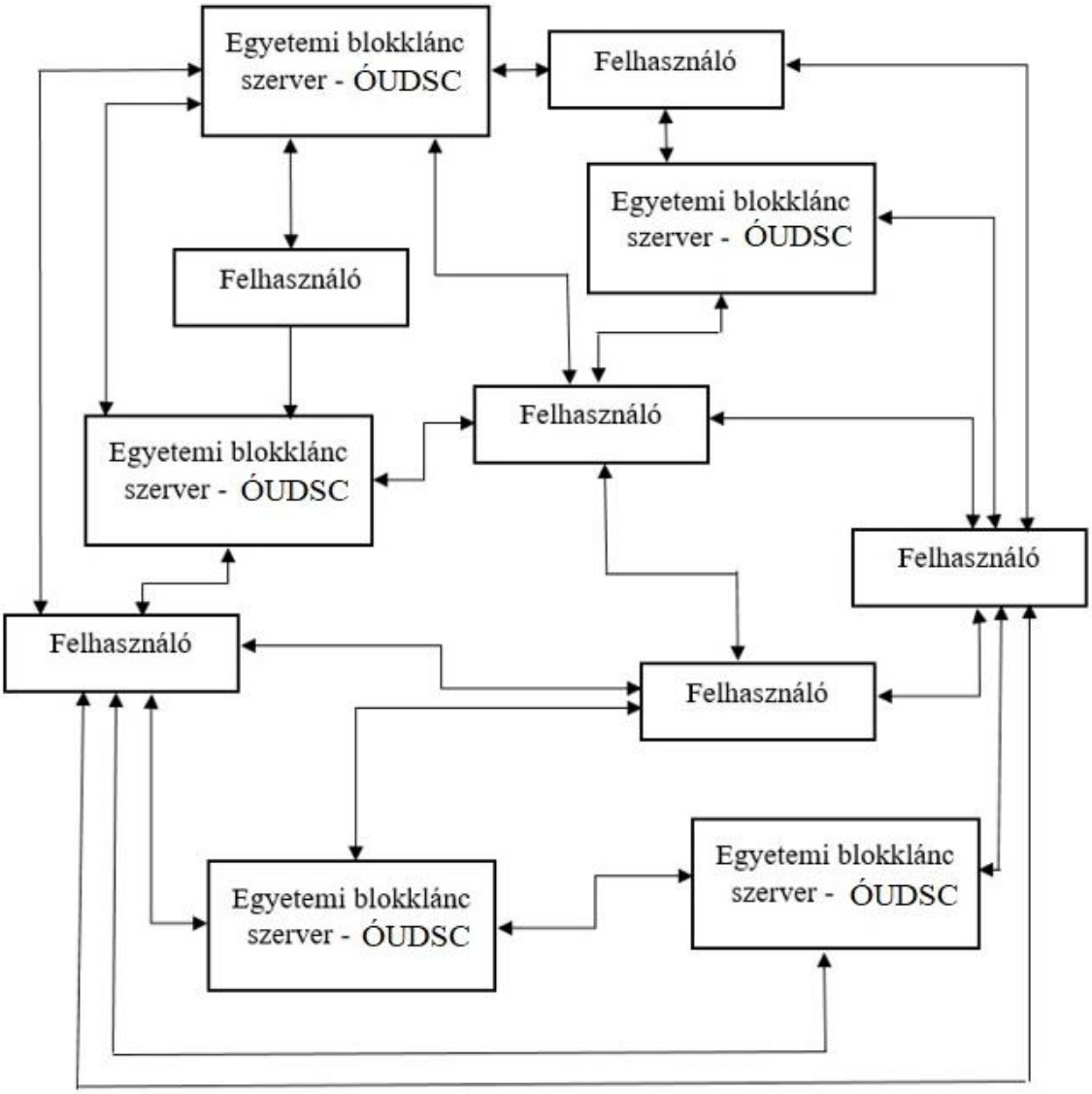
Megadtam ehhez a csatlakozási engedélyt:

universitychain ÓUDSC támogatás: 192.168.0.2 kapcsolódás.

4. ábra. ÓUDSC blokklánc létrehozása [93]

Mint ahogyan a fenti ötödik táblázatban látható az egyetemi blokklánc minden egyes blokkmérete 1MB lesz. Ajánlatos ezt a méretet alkalmazni, mivel így a blokkok gyorsak maradnak a méretükből

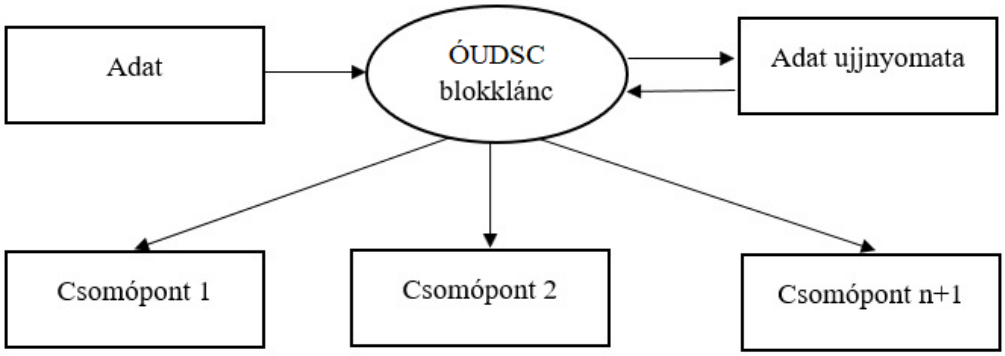
kifolyólag, így a kamerafelvételek adatai is könnyebben feltölthetőek. További előny, hogy még kisebb sávszélesség esetén is a teljes blokklánc gyors marad. A blokklánc struktúrájából adódóan több szerver nagyobb biztonságot nyújt. A blokklánchoz egyébként nem csak az egyetemi felhasználókat lehet hozzárendelni, hanem egyéb felhasználókat is. Ezt az oktatási intézménynek, illetve a rendszergazdának kell jóvá hagynia. Az alábbi ábrán az ÓUDSC decentralizált blokklánc adattárolási megoldását mutatom be:



5. ábra. ÓUDSC decentralizált blokklánc alapú egyetemi adattárolási rendszer (szerkesztett) [94]

Miután a fentebb bemutatott módon létrejött a genezis blokk (ez a blokklánc első blokkja) a további blokkok már képesek adatokat fogadni az NVR egységtől. Az adatokat a blokklánc ujjnyomatokkal látja el, ez által tovább lehet növelni az adatok biztonságát. Ezt követően az adatok a csomópontokban kerülnek tárolásra. Minél több csomópont található a blokkláncban, az annál biztonságosabb. A cél, hogy minél több csomópont tárolja el a felvételek feldarabolt részeit. Mint a fenti ábra is szemlélteti, az ÓUDSC blokklánchoz több felhasználó is csatlakozhat. A felhasználók hozzáférését az okos szerződésen keresztül szabályoztam.

Az adatok hozzáféréséhez a blokkláncon belül az adatok ujjlenyomatára is szükség van. A hatodik ábra az ÓUDSC blokklánc egyetemi struktúráját ábrázolja.



6. ábra. Egyetemi ÓUDSC blokklánc struktúra [5]

5.2 Okos szerződés alkalmazásának lehetősége az egyetemi adattárolás területén

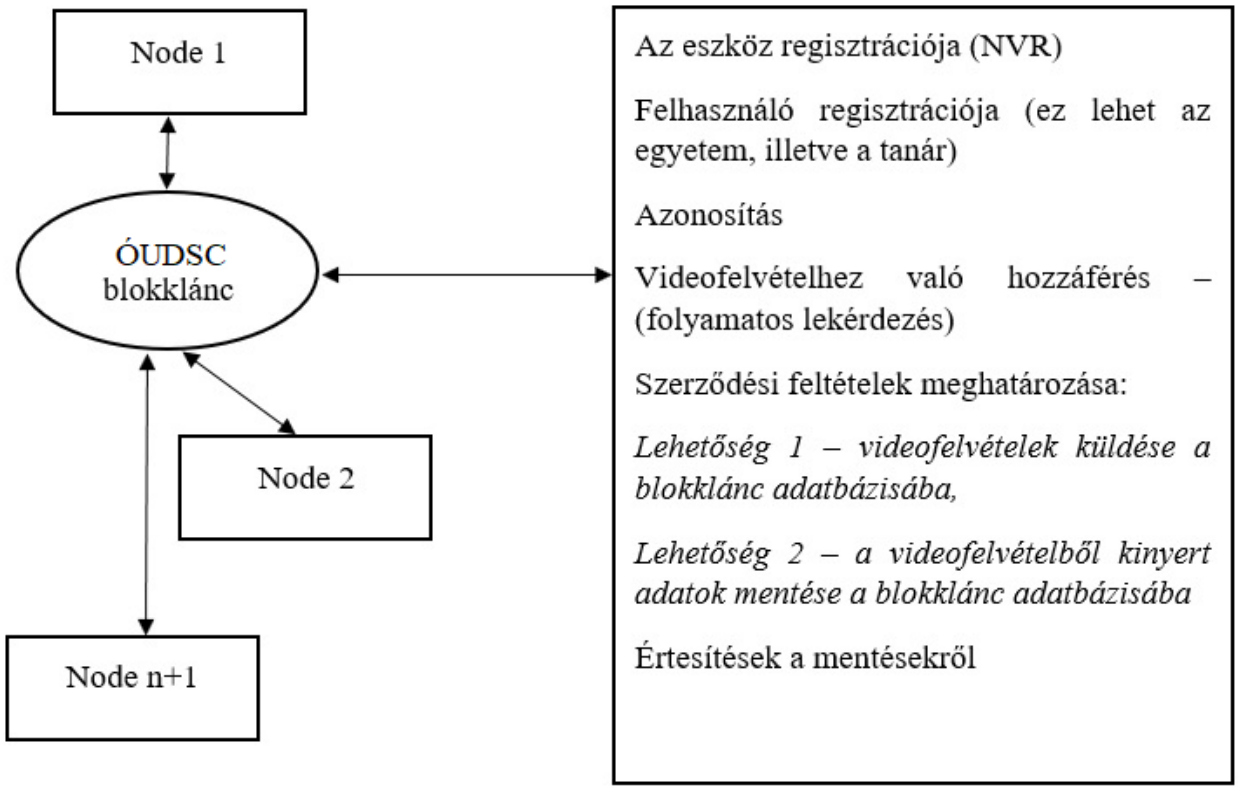
Annak érdekében, hogy a jelenléti ívkészítő rendszer automatizáltan működjön okos szerződést alkalmaztam.

Az okos szerződések jellemzője, hogy képesek az adatok rögzítésére a blokklánc felhasználása által egy adott esemény bekövetkezésekor. Ezeket az eseményeket előre meghatározzák és a programkód automatikusan végrehajtja azokat. [95]
Az oktatási intézmény esetében a felhasználó és az NVR regisztrációja után az okos szerződés automatikusan elmenti a beérkező adatokat a blokkláncba, illetve hozzáférést biztosít ahhoz.

Az okos szerződések által adott a lehetőség akár az adatfájlok automatizált cseréjére is. Hátránya, hogy a szerződés nem tudja leellenőrizni az adatfájlok tartalmát, mivel azok titkosítottak. Ez

azonban kiküszöbölhető egy értékelés alapú megoldással. Ilyen az a pontozási rendszer, amelyet az EBay is alkalmaz. Ha valakit lepontoznak, akkor az a továbbiakban megbízhatatlannak számít és mellőzni fogják. A rendszer legnagyobb gyengesége az lehet, ha a bányászok összefognak és közösen megtámadják a saját rendszerüket. E lépés következtében az okos szerződések elveszthetnek, mivel azok a blokkokban kerülnek tárolásra. [96] Az okos szerződésekben a felek megőrizhetik anonimitásukat. [97]

Az ÓUDSC blokklánc esetében az okos szerződéshez szükséges adatokat az ÓUDSC blokkláncból nyertem ki. Ezt az alábbi hetedik ábra prezentálja.



7. ábra. Az okos szerződés összekapcsolása az NVR egységgel [93]

A gyakorlati megvalósítás részeként az okos szerződést összekapcsoltam az NVR egységgel, így a hozzáféréseket hatékonyan tudtam kezelni. Ez által a lekérdezést, illetve a hozzáférési szabályozást a szerződés algoritmusával végeztettem el. Ezeket a beállításokat az alábbi nyolcadik ábra szemlélteti:

```
function hozzáférés (Óbudai Egyetem NVR)
Input: lekérdezés (Óbudai Egyetem NVR)
Output: megadott, megtiltott
 if üzenet (Óbudai Egyetem NVR) létezik & lekérdezés (Óbudai Egyetem NVR) érvényes then
     videókamera engedélyezve/megtagadva
          if az Óbudai Egyetem NVR be van jegyezve a megadott listában then
               felhasználó ID ellenőrzése
                if felhasználói ID elérhető = hozzáférés megfelelő then
                    visszatérés megadva
               else
                visszatérés megtagadva
                end if
              else
             visszatérés megtagadva
           end if
else
   visszatérés megtagadva
end if
end function
```

8. ábra. Okos szerződés algoritmusa a felhasználói hozzáférés biztosításához [93] [98]

5.3 Automatizált elektronikus blokklánc alapú hallgatói jelenléti ív működésének sémája

Miután létrehoztam a blokkláncot az NVR és a biztonsági kamera analitikai funkcióihoz kellett visszatérnem, mivel a kamerarendszernek ismernie kellett a hallgatói listát. Ez a következő elemekből tevődött össze:

- Név és vezetéknév,
- Évfolyam,
- Képzés megnevezése (milyen képzésben vett részt a hallgató).

A csoportosítás nagyobb átláthatóságot biztosított a hallgatók között. Ez azért előnyös, mivel több száz hallgató regisztrációja történik meg egyszerre és ilyen esetben az adatbázis áttekinthetősége szükségszerű.

A hallgatói lista betáplálása után az arcképek hozzárendelése következett. Célszerű, hogy ezek a képek jó minőségűek és nagy felbontásúak legyenek. Erre azért van szükség, mivel a biztonsági kamera mesterséges intelligenciája ezt a képeket hasonlítja össze a hallgatók arcképével.

A soron következő adat, amelyet meg kell adni a kamerarendszernek az a tantermek száma, illetve azok megnevezése. Ez azért szükséges, mivel az azonosítás a tantermek bejárati ajtajainál történik.

Az órarendek hozzáadása a kamerarendszer adatbázisához az egyik legidőigényesebb adminisztratív feladat, mivel az szemeszterenként változik. Az órarendek hozzáadása által tudni fogja a kamera, hogy a hallgató milyen tanórán tartózkodik és melyik tanteremben. Az adminisztratív feladat csökkentése érdekében az órarendet ajánlatos szinkronizálni egy olyan adatbázissal, ahol ez az adat megtalálható, így nem szükséges azokat egyesével bevinni.

Ahhoz, hogy a biztonsági kamera felismerje a hallgatókat arcdetektálásra van szükség, mivel csak így képes felismerni és megkülönböztetni az arcot a többi emberi testrésztől.

Az arcdetektálás után az arcfelismerő funkciónak köszönhetően a kamera fel fogja ismerni a hallgatót a megadott kép alapján. Minél több alkalommal kell hallgatót azonosítania, annál több metaadattal rendelkezik és így válik egyre hatékonyabbá.

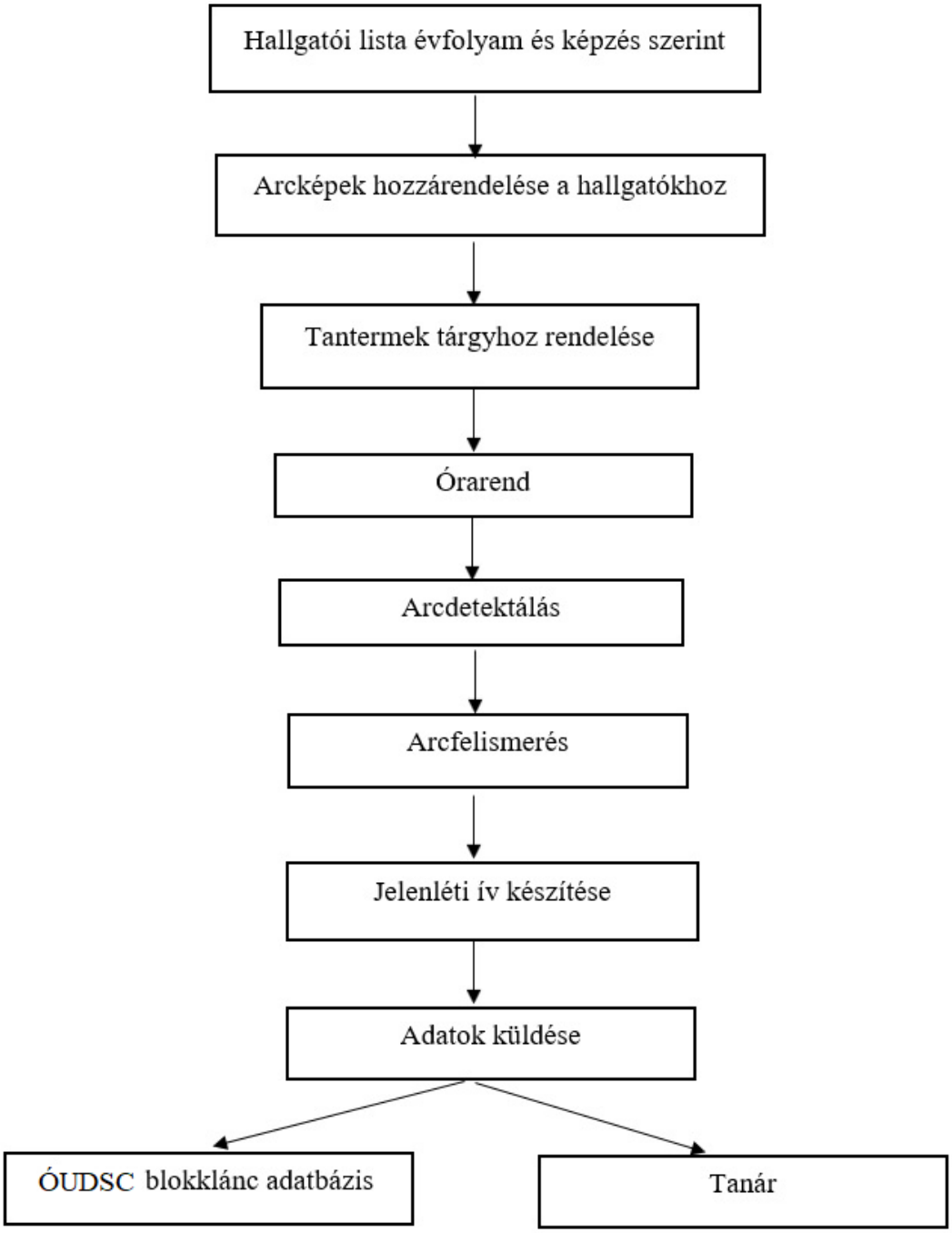
A hallgatók azonosítása, valamint a tanterem meghatározása után az órarend figyelembevételével a kamerarendszer tudni fogja, hogy mely hallgatók vettek részt a tanórákon. A felsorolt adatok birtokában el fogja készíteni a jelenléti ívet.

Utolsó lépésként az adatokat elküldte a megadott email címre. Az adatok küldése történhet:

- Naponta,
- Hetente,
- Havonta,
- Szemeszterenként.

Érdemes a napi adatküldést választani a biztonság fokozása érdekében.

Az elektronikus jelenléti ívet készítő biztonsági kamerarendszer működésének sémáját az alábbi kilencedik ábra szemlélteti.



9. ábra. Hallgatói jelenléti ív készítésre alkalmas kamerarendszer struktúrája [76] [93]

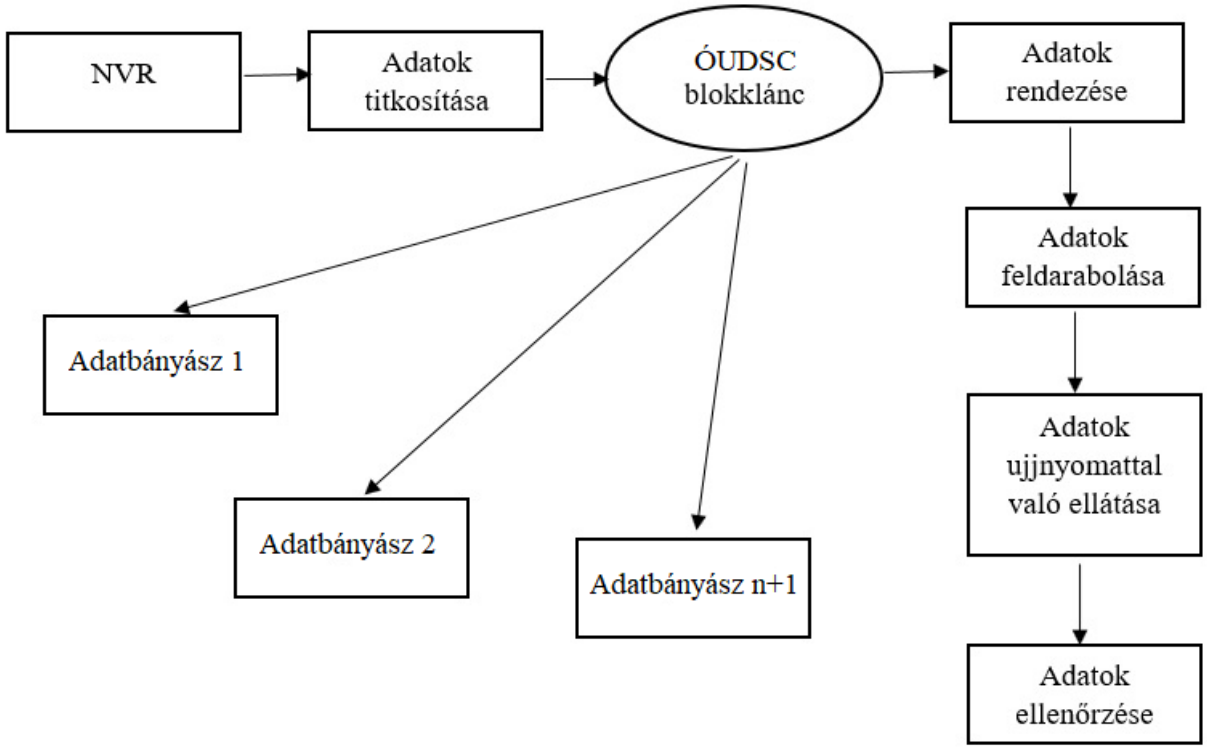
A biztonsági kamera két különböző adatot rögzít:

- Biztonsági felvételt, amennyiben mozgást érzékel,
- Jelenléti ívet.

Mind a két típusú adatot küldés előtt titkosítani kell, hogy azok ne kompromitálódhassanak. Az adatok rendezése több részből állt, úgy mint:

- Adatok feldarabolása,
- Adatok ujjnyomattal való ellátása,
- Adatok ellenőrzése.

Amennyiben a visszaellenőrzés során az adatokkal minden rendben van, úgy az ÓUDSC blokklánc az adatokat elküldi az adatbányászok számítógépeire tárolás céljából. A biztonsági kamerarendszer és a blokklánc közötti kapcsolat modell a tizedik ábrán figyelhető meg.

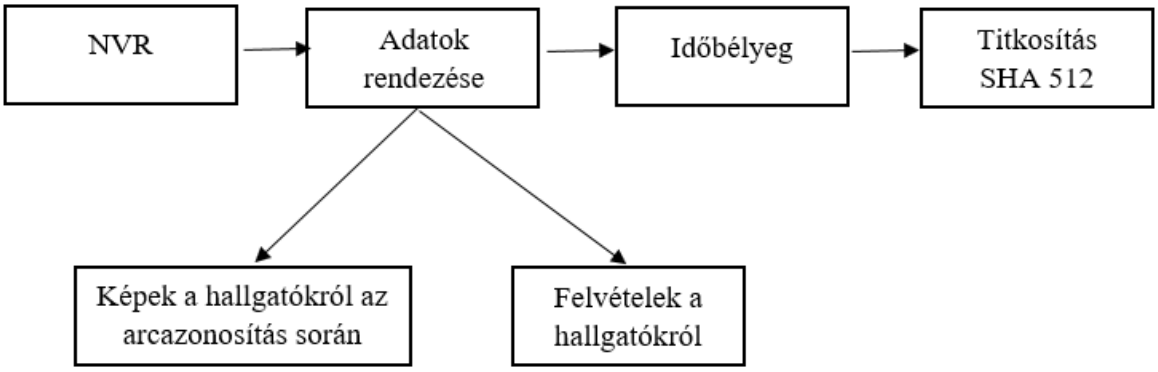


10. ábra. A biztonsági kamerarendszer és a blokklánc közötti kapcsolat modell

Az adatok elküldése és titkosítása előtt a hallgatókról készült felvételt időbélyeggel kell ellátni. Erre azért van szükség, hogy mindenki számára elfogadható bizonyítékként szolgálhasson az a kép, amely azt állítja, hogy a hallgató az adott időpontban az adott tanteremben tartózkodott. Kizárólag az időbélyeggel ellátott képeket lehet bizonyítható erejűnek tekinteni. Amennyiben ez hiányzik, illetve az azonosítás sikertelen, úgy a rendszernek jeleznie kell, hogy az azonosítás nem sikerült. Ilyen esetben az oktatónak kell az azonosítást elvégeznie, felülbírálnia, illetve

jóváhagynia azt. Ha az azonosítást a rendszer automatikusan nem végezi el, hanem külső segítség igénybevétele által, úgy az időbélyegre továbbra is szükség van.

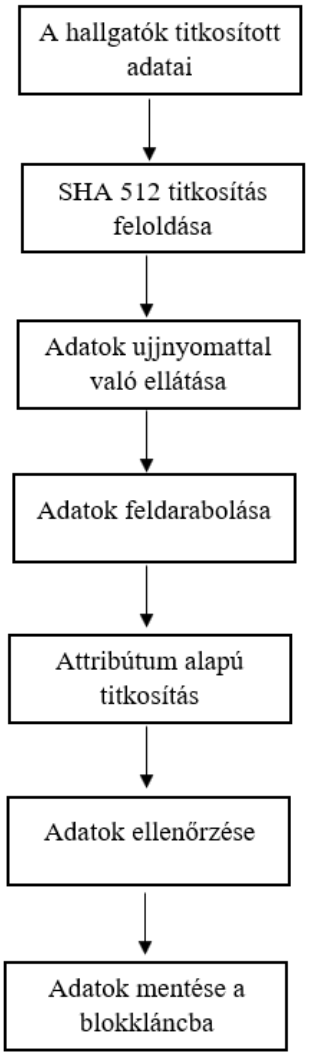
Nem csak a hallgatókról készült képet kell időbélyeggel ellátni, hanem a biztonsági felvételeket is. A biztonság további fokozása érdekében az adatokat szükséges titkosítani az időbélyeg alkalmazása mellett. Az alábbi ábra ennek menetét prezentálja.



11. ábra. Az adatok időbélyeggel való ellátása a titkosítás előtt

Az adatok titkosítása az SHA 512 függvénnyel történik. Ezt az Egyesült Államok Nemzeti Szabvány és Technológia Hivatala (NIST) szabványosította, amelyet az NSA (National Security Agency - Nemzetbiztonsági Ügynökség) tervezett. Az SHA-2 algoritmusok 2001-ben jelentek meg először a FIPS PUB 180-2 számú dokumentumban. Az SHA512 esetében a számok 64bit hosszúságúak, a fő ciklus 80 körből áll, a blokkméret pedig 1024bites. [99]

A blokklánc működése szorosan kapcsolódik a hash függvényekhez. Amikor valaki új adatot szeretne tárolni, akkor az új blokk a blokklánc végére kerül. Az NVR már titkosítva küldi az adatokat a blokkláncnak. A blokklánc mivel SHA512 algoritmust használ és ABE (Attribute-Based Encryption – Attribútum alapú titkosítást) is ismeri (ez a privát blokkláncok jellemzője), ezért azokat vissza tudja fejteni az adatbányászok segítségével. Lényeges szempont, hogy az adatok az NVR és a blokklánc közötti útvonalon is biztonságban legyenek, valamint, hogy a tárolás során is megfelelő titkosítási módszer legyen alkalmazva. Az SHA 512 algoritmus biztosítja, hogy az NVR és a blokklánc közötti útvonalon az adatok ne sérülhessenek, valamint, hogy azokhoz illetéktelenek ne férjenek. Az alábbi ábra a jelenléti ívet készítő rendszer adatbiztonsági megoldását prezentálja.



12. ábra. A hallgatói jelenléti ívet készítő rendszer adatbiztonsági megoldása

Az ABE célja, hogy az adatokhoz csak az férhessen hozzá, akik arra jogosultak. Ez a titkosítási metódus az IBE (Identity Based Encryption – Azonosító alapú titkosításon) alapszik. A módszer lényege, hogy a felhasználó személyes adatát, amely lehet akár digitális fénykép, IP-cím, illetve ujjnyomat használja nyilvános kulcsként az adatok titkosítására.

A nyilvános kulcsú titkosítás általában a következő módon működik. A fogadó félnek rendelkeznie kell a nyilvános-privát kulcspárral, továbbá a rejtő és a fejtő kulcsot is egyszerre kell létrehoznia. Mindennapi életben ezzel kapcsolatban felmerül egy kérdés. A küldő fél honnan tudja biztosan, hogy a nyilvános kulcs a minden bizonnyal a fogadóé? Ebben nyújt segítséget a PKG (Privat Key Generator – Privát Kulcsú Generátor), amely privát és nyilvános kulcsokat hoz létre. A PKG

feladata, hogy titkosítja az adatot a nyilvános kulcs segítségével. Ezt követően a fogadó félnek hitelesítenie kell magát a PKG irányába, így a mesterkulcs alkalmazása által kap egy privát kulcsot, amellyel meg tudja fejteni az adatot.

Az IBE alkalmazása során azonban nem kell az adatot fogadó félnek nyilvános-privát kulcspárral rendelkeznie, helyette elegendő egy meghatározott személyi azonosító adatt. A kulcspárok generálása időben függetlenül történik. A fejtő kulcs generálása történhet akkor, amikor arra a fogadó félnek szüksége van, ezért nincsen szükség költséges nyilvános kulcsú infrastruktúrára. [100]

Az ABE esetében a visszafejtési kulcsba be lehet ágyazni hozzáadott paramétereket. Ilyen lehet, akár az is, hogy a küldő fél meghatározhatja, hogy fogadó fél mikortól férhet hozzá az adatokhoz, így a helyes kulcsot az adott időpontban fogja megkapni. Továbbá a nyilvános kulcsokat az attribútumok listájából készítik. A nyilvános kulcsok alkalmazása helyett, bárki, aki rendelkezik a megfelelő attribútumokkal, hozzáférhet az adatokhoz. Az ABE esetében hatékonyan lehet szabályozni, hogy kik legyenek azok a személyek, akik hozzáférhetnek azokhoz. [101]

5.4 A jelenléti ívet készítő rendszer fontosabb konfigurálási állomásai

Minden bizonnyal az egyetemi privát blokkláncot egy informatikus, vagy programozó fogja létrehozni, mivel ez komoly szaktudást igényel. A rendszeres blokklánc használathoz azonban nincsen szükség magasan képzett informatikus szakemberre. A másodlagos konfigurációs beállításokat már egy laikus is el tudja végezni. A primáris konfigurációs beállításokhoz a következők tartoznak:

- A blokklánc csomópontjai nagyságának meghatározása,
- A működéshez szükséges szerver, illetve szerverek létrehozása,
- Blokklánc összekapcsolása az NVR egységgel,
- Okos szerződés megírása.

A másodlagos konfigurációs beállításokat két részre bontottam. Az első az NVR a második pedig a blokklánc konfigurálása volt. Az NVR beállításaihoz tartozik:

- A kamerákat mozgásérzékelésre állítottam. Amennyiben mozgás történik a felvétel automatikusan elindul.

- A kiválasztottam a kívánt SHA 512 titkosítási eljárást az NVR egységben. A titkosítás bekapcsolása nélkül az adatok nincsennek biztonságban.
- Meghatároztam azt, hogy az adatok küldése a blokkláncba milyen időközönkét történjen,
- Elvégeztem a tűzvédelemmel kapcsolatos beállításokat. Beállítottam, hogy a kamera milyen hőmérséklet emelkedésre riasszon. Tűz esetén ajánlatos az azonnali adatküldés lehetőséget kiválasztani.

A blokkláncba történik minden fontosabb adat mentése, ezért a blokkláncra, mint érzékeny adatok tárhelyére tekintettem, amelyet kellő elővigyázatossággal használtam. Az alábbi teendők tartoztak a blokklánchoz:

- Az elmentett adatok időszakos ellenőrzése. Figyelemmel kísértem, hogy az adatokat az NVR egység meghatározott időközönként elküldi-e?
- A blokklánchoz való jogosultságokat kiosztottam. Új felhasználókat rendeltem a blokklánchoz, valamint szükség esetén töröltem a meglévőket.
- A blokklánc helyes működését rendszeresen ellenőriztem, mivel az adatok a nap 24 órájában rendelkezésre kellett, hogy álljanak.

A rendszer folyamatosan karbantartást igényelt. Az NVR egység szoftverét frissítettem. Minden kamera hibátlanul kellett, hogy működjön, mivel rendszerleállás esetén a jelenléti ív készítése szünetelt. Az oktatási intézmények számára célszerű egy kellően erősségű szünetmentes táp beszerzése áramkimaradás esetére.

5.5 Jelenléti ívkészítő kamerarendszer a tűzvédelemben

Az ÓUDSC jelenléti ívkészítő kamerarendszer tulajdonságainak köszönhetően az a tűzvédelemben is alkalmazható. A már meglévő tudása hozzájárul ahhoz, hogy az oktatási intézmények egy új modern megoldással bővítsék a jelenleg alkalmazott tűzvédelmi rendszerüket. A kamera név szerint azonosítja a hallgatókat, ezért az precízebb nyomon követést és azonosítást tesz lehetővé. Egy lehetséges evakuáció során fontos, hogy mindenki elhagyja az épületet. Egy „eltévedt” hallgató gyors megtalálása és kimenekítése kulcsfontosságú az emberi élet megóvásában.

A következő lehetséges negatív tényezők lehetnek hatással arra, hogy a hallgató ne tudja elhagyni az oktatási intézményt időben:

- Hirtelen jött pánik és ijedtség következményeként a hallgató nem tud racionális döntéseket hozni, ezért nem látja át a helyzetét kellőképpen,
- A gyors tűz és füst terjedés megakadályozhatja az evakuációs útvonal megtalálását,
- Sebesülés miatt a mozgása korlátozottá vállhat, így akár életveszélyes helyzet is kialakulhat.

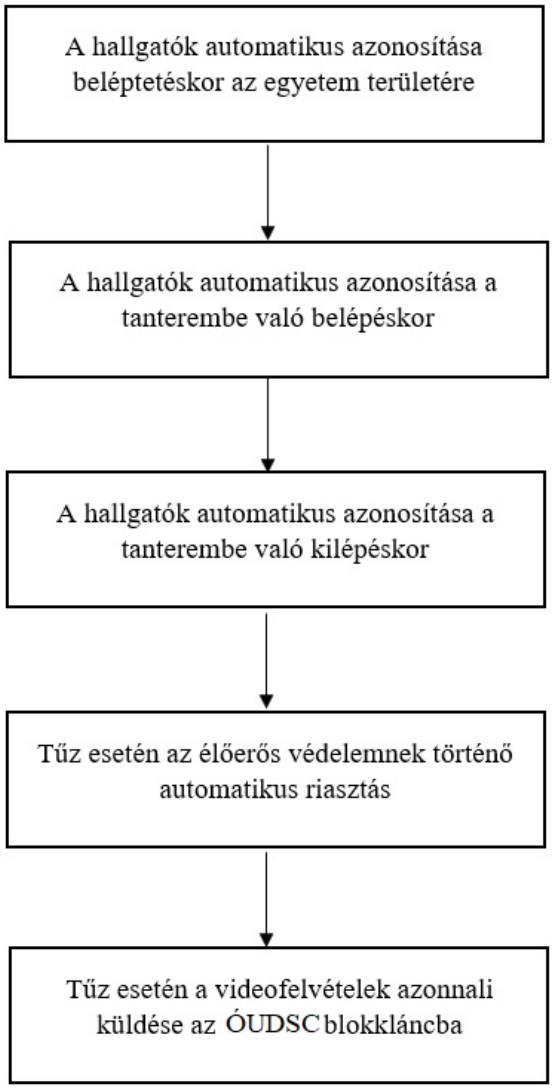
A kamerarendszer a következőképpen segíti a mentőalakulatok dolgát:

- Információval szolgál a hallgatók aznapi létszámával kapcsolatban, így az oktatási intézményben tartózkodó pontos létszámot meg tudja határozni,
- A tűzoltók kiérkezésekor azonnal információt nyújt a hallgatók tartózkodási helyéről,
- Képes a hallgatókat név szerint azonosítani,
- Amennyiben a kamerarendszer nem sérül a tűz következtében, úgy folyamatosan képes nyomon követni annak terjedését,
- Tűz esetén riasztja az előerős védelmet, így akár időben megakadályozható a tűz terjedése,
- Felvételt készít a tűzesetről, amelyet a blokkláncban biztonságosan eltárol, ezzel is segítve a tűzvizsgálók dolgát.

Tűz esetén a felvételek biztonságos tárolása fontos szempont. A mentés elsődlegesen az NVR merevlemezére történik és csak ez után kerülnek az adatok a blokkláncba. Javaslom a heti rendszerességű biztonsági mentéseket alkalmazni. Tűz esetén azonban a felvételek a merevlemezen veszélybe kerülhetnek, ezért a beállított heti mentéseket felül kell bírálni. Ilyen esetben az adatok küldését rögtön el kell kezdeni, mivel veszélybe kerülhet:

- A hallgatók óralátogatásával kapcsolatos lista,
- A hallgatókról készült felvételek, amelyek a helyesen elkészített jelenléti ív bizonyítékául szolgálnak,
- A tűzesetről készült felvétel, amely a későbbiekben fontos lehet az oktatási intézmény, illetve a tűzoltóság és a rendőrség számára is.

Az alábbi ábra a jelenléti ívkészítő kamerarendszer működési sémáját mutatja be a tűzvédelem részeként:



13. ábra. A jelenléti ívet készítő kamerarendszer működési sémája a tűzvédelem részeként

5.6 Az NVR egység összekapcsolása a biztonsági kamerákkal, valamint a blokklánccal

Ahhoz, hogy a gyakorlatban a blokklánc adatbázis hibátlanul működjön annak számos elemére oda kellett figyelnem. Első lépésként a biztonsági kamerákat kellett összekapcsolnom az NVR egységgel, hiszen ez az egység biztosítja a kamerák működését. A következő felsorolásban azokat a buktatókat emelem ki, amelyeket a tesztidőszak során tapasztaltam. Ezek a következők voltak:

- A teszt időszakban egy 4 portos NVR egységre volt szükségem, mivel 3 különböző tudású biztonsági kamerát használtam. Az oktatási intézményeknek ajánlatos a 24 portos NVR

egységen elgondolkodniuk, mivel ez meghatározza a telepíthető kamerák számát. Fontos előre kalkulálni a biztonsági kamerák számával és csak utána kiválasztani a megfelelő NVR egységet.

- A tömörítési lehetőségek kiválasztására is érdemes odafigyelni. A H.264 szabvány által már elfogadható tömörítés hatékonyságot tudtam elérni, azonban a leghatékonyabb megoldást a H.265 szabvány biztosítja. Alkalmazása által értékes tárhelyet tudtam megtakarítani.
- Az Internet sávszélességét is annak jövőbeli sebességét ajánlatos már jó előre számításba venni. A tesztidőszakban elsőként egy olyan NVR egységre esett a választásom, amely lassabb Internet sávszélességet támogatott, mint amellyel az oktatási intézmény rendelkezett. Az NVR által támogatott sávszélesség 80 Mbps (Megabit per secundum - Sávszélesség/adatátviteli sebesség mértékegysége) volt, míg az egyetemi Internet sebesség 150 Mbps. Ebből kifolyólag a teljes rendelkezésre álló sávszéllességet nem tudtam maradéktalanul kihasználni. Az NVR cseréje után az adatkommunikáció gyorsabbá vált, így már sikerült elérnem a 150 Mbps sebességet WiFi kapcsolaton keresztül. A teszt során észrevettem, hogy az NVR által támogatott LAN, illetve WiFi sebesség eltérő lehet. Erre érdemes külön figyelmet fordítani.
- A maximális HDD kapacitás portonként meghatározza, hogy egy portra mekkora kapacitású merevlemezt lehet csatlakoztatni. A gyakorlatban 1TB (terabyte – adathordozó mértékegysége) nagyságú merevlemezekre esett a választásom. A 3 kamerából álló kiépítéshez ez bőségesen elegendőnek bizonyult. 24 kamera esetén értelemszerűen ennél nagyobb kapacitásra van szükség. Hosszútávú alkalmazás esetén javaslom a 4TB-os merevlemezek alkalmazását.

Célszerű az NVR felhasználói felületén az adatok másodlagos mentési helyének a blokkláncot megadni, illetve annak pontos IP címét. Részleteiben a következő adatok kerültek mentésre a blokklánc adattárában a megvalósítás során:

- Hallgatókról készült fényképek,
- Hallgatókról készült videófelvételek,
- Hallgatók órarendje a tantermi beosztásokkal együtt. [74]

5.7 Kamerák által generált adatmennyiségek

Gyakorlati megvalósításom során a kamerák telepítése 3 fázisban történt. Ez a következőképpen nézett ki:

- Először a HD felbontással rendelkező kamerákat szereltem fel és próbáltam ki,
- Ezt követően a 2 MP kamerák következtek,
- Nem utolsó sorban pedig napjaink egyik legmodernebb 10 MP biztosági kamerái váltak a teszt részeseivé.

A tesztelés alatt a lehető leghatékonyabb tömörítési eljárás alkalmaztam, mégpedig a H.265 szabványt. A kapott eredmények alapján a következő megállapításokra jutottam:

- A HD felbontással rendelkező biztonsági kamerák megfelelő minőségű videófelvételeket készítenek. A nagyobb felbontás lényegesen nagyobb adatmennyiséget generált, amely a mindennapok során inkább problémát jelentett, mintsem előnyt. A HD felbontás azért bizonyult elegendőnek, mivel ezek a kamerák zárt térben kerültek telepítésre, ahol nincsenek nagy távolságok. A kamerák a tantermek bejárati ajtaja elé kerültek felszerelésre, így az előttük elhaladó hallgatókról megfelelő minőségű felvételeket tudtak készíteni.
- A 2 MP-es kamerák már sokkal nagyobb adatmennyiségeket generáltak, valamint az arcfelismerő hatékonyságuk is növekedett.
- A 10MP-es biztonsági kamerák elképesztő részletességgel rögzítették a felvételeket. Feltételezhetően ezeknek a széleskörű alkalmazása az oktatási intézményekben egyelőre a távoli jövőképet jelenti, mivel a magas áruk akadályozza az elterjedésüket. A legnagyobb problémát azonban az az adatmennyiség jelentette, amelyet napi szinten generáltak. Jelenleg a hatalmas adatmennyiségek tárolása az oktatási intézmények számára nehézséget jelent.
- Ezen felül számításba kellett vennem a megnövekedett adatforgalmat is, mivel azok jelentősen leterhelték az egyetem Internet hálózatát. Ez főleg a 10 MP-es kamerákra volt jellemző. Az adatok továbbítását a blokkláncba az esti időszakban javasolom, amikor nincsen más adatforgalom az oktatási intézményben. [74]

A negyedik táblázat a biztonsági kamerák által generált adatmennyiségeket szemlélteti:

Felbontás	Tömörítési eljárás	Kamerák száma	Napok száma	Napi órák száma	Hálózati sávszélesség	Adat-mennyiség
1.3MP (HD)	H.265	3	5	12	150 Mbit/s	470 GB
2MP (1080p)	H.265	3	5	12	150 Mbit/s	710 GB
10 MP	H.265	3	5	12	150Mbit/s	1.2TB

4. táblázat. A biztonsági kamerák által generált adatmennyiség a gyakorlatban [74]

A gyakorlati kutatásom során törekedtem a precizitásra, valamint, hogy részleteiben feltárjam a kamerák képességeit. A teljes tesztidőszak 6 hétig tartott, továbbá mind a három kameratípusra 2 hét tesztidőszak jutott.

Fontos megjegyeznem, hogy ezek a kamerák kivétel nélkül mind mesterséges intelligenciával rendelkeztek. Mivel a tesztelés az oktatási intézményben történt, ezért a felmérésem során olyan arcfelismerést nehezítő körülményeket tártam fel, amelyek negatívan hatottak ki az azonosítás sikerességére [88]. Ezek a következők voltak:

- Az arc takarása a tanterembe való belépéskor. Ez azért fordulhatott elő, mivel a hallgatók szinte egyszerre egyazon időpontban lépnek be a tantermekbe. Ez megnehezítette az azonosítást,
- A kamerákat megfelelő magasságban és szögben kellett elhelyezni. Miután ez megtörtént a hibás azonosítások száma csökkent. Az első telepítés során a fényvisszaverődésre nem lett kellő figyelem fordítva, ezért a kamerák helyzetét módosítani kellett,
- Az eltérő öltözködési stílusok negatívan hatottak ki a kamerák hatékonyságára. Télen a sapka és a sál akadályozó tényezőnek bizonyult.

A kutatásomban 57 hallgató vett részt, akik Informatika 1 tárgyat hallgattak. Ez a gyakorlatban 3 csoportot jelentett. Fontos szempont volt, hogy mind a 3 kamera esetében ugyanazok a hallgatók vegyenek részt, így adott volt a lehetőség a kamerák azonosítási képességeinek és azok pontosságának a meghatározására. A hat hetes időszak 2020 január közepétől egészen február végéig tartott. Fontos volt, hogy a tesztidőszakban a kamerák rögtön egymás után kerüljenek

alkalmazásra. A téli tesztben a hallgatók öltözködési szokásai, illetve frizurájuk hasonló volt a megfigyelt időintervallumban. Amennyiben a kamerák egy része télen a másik része pedig nyáron lett volna tesztelve, úgy az azonosítás pontosságában nagyobb eltérések mutatkoztak volna, amelyek negatívan hatottak volna ki a mérés pontosságára. [74] Az azonosítás során kapott eredményeket az ötödik táblázat szemlélteti:

Kamerák csoportosítása felbontásuk alapján	**Pontos hallgatói létszám azonosítás az első héten**	**Pontos hallgatói létszám azonosítás a második héten**
1.3 MP (HD) kamera	43	51
2 MP (HD) kamera	46	52
10 MP kamera	51	55

5. táblázat. A kamerák azonosítási hatékonysága a gyakorlatban [74]

Mint látható a kamerák a második héten hatékonyabban működtek, mint az azt megelőző héten. Ez a beépített mesterséges intelligenciának köszönhető. A kamerák folyamatosan tanultak, így az azonosítás hatékonysága jelentősen javult a tesztidőszak végére. A kapott eredmények alapján kijelenthető, hogy:

- Az 1.3 MP-es kamera esetében az első héten 75%-os pontossággal azonosította a hallgatókat, addig a második héten már a hallgatók 89%-át ismerte fel.
- A 2 MP-es kamera az első héten 80%-os hatékonyságot tudott elérni, míg a következő héten már 91%-os pontossággal működött.,
- Nem utolsó sorban pedig a 10 MP-es kamera 89%, illetve 96%-os pontosságot tudott elérni.

Feltételezhetően a nagyobb pixelsűrűség kihatással van az azonosítás hatékonyságára, azonban a válasz ennél bonyolultabb. A pixelszám növekedésével a kamerákban található processzor erőssége is arányosan növekedett. A továbbiakban vizsgálni lehetne a beépített mesterséges intelligencia szoftverek közötti eltérést is, azonban a gyártó ezeket az információkat nem tüntette fel a csomagoláson, valamint a honlapján is hiányoztak ezek az adatok.

Az NVR és a blokklánc közötti kapcsolat sikeresen ki lett építve így az adatok mentése a blokkláncban megtörtént. A csomópontok elmentették az adatokat (ez alatt értendő a videófelvételek és a fényképek mentése is) azonban ez a vártnál sokkal hosszabb ideig tartott. A hagyományos felhő alapú rendszerek ennél azért gyorsabbak. Erre a kérdésre a válasz feltételezhetően az lehet, hogy a blokkláncok akkor vállnak igazán hatékonyá, ha azok minél több számítógépen futnak. A kutatás idején ez mindössze két számítógépet jelentett. [74]

6 EMPIRIKUS KUTATÁS I

6.1 A kutatás során alkalmazott módszerek

Módszertanilag a kutatásom a szakirodalmi feldolgozáson, statisztikai adatok elemzésén, valamint a saját kutatási eredményeken alapszik. A kutatásomban alkalmazott módszerek alkalmasak arra, hogy feltárják az oktatók és a hallgatók meglátásait a tanórai online jelenléti ívkészítés fontosságáról. Továbbá a kutatásom meghatározó részét képezi az is, hogy megvizsgáljam azt, hogy a hallgatókat mennyire zavarja az ő azonosításukra képes kamerarendszer, amely folyamatos megfigyelésre alkalmas.

A kutatásom során kvantitatív kutatási módszert alkalmaztam. A kvantitatív vizsgálathoz a kérdőívem szolgált segítségül, mely a társadalomtudományos vizsgálódás hasznos eszköze. [102]

A kérdőívem nyitott és zárt kérdéseket tartalmazott. A zárt kérdések esetében előre rögzített válaszlehetőségek álltak a rendelkezésre. Likert-skálát alkalmaztam abból kifolyólag, hogy az állítással való egyetértés mértékét, illetve a vélemény helyeslését részleteiben megvizsgálhassam. A zárt kérdések esetében könnyen számszerűsíthető és statisztikai módszerekkel elemezhető a vizsgálni kívánt terület. A nyitott kérdésekre a válaszokat a megkérdezettek szabadon fogalmazhatták meg, így azokra a kérdésekre is választ kaphattam, hogy a válaszadóknak milyen tapasztalataik vannak a „hagyományos” papíralapú jelenléti ívvel kapcsolatban a tanórákon?

A kérdőívem megszerkesztése során törekedtem a rövid, könnyen értelmezhető és áttekinthető forma kialakítására. A zárt kérdések esetében az online kérdőívemben a válaszokat ikszeléssel lehetett megválaszolni, nyitott kérdések esetében viszont elegendő helyett biztosítottam a szabadon megfogalmazható válaszadásra és gondolat kifejtésre.

A kutatásom első részében az egyetemi hallgatók nézőpontjait és meglátásait vizsgáltam az online automatizált elektronikus blokklánc alapú hallgatói jelenléti ívkészítő rendszerről.

6.2 Kutatásban részt vett hallgatók eloszlása oktatási intézményenként

A hatodik táblázat a kutatásban részt vett hallgatókat, illetve oktatási intézményeket szemlélteti együttesen:

Ország	Oktatási intézmények	Hallgatók létszáma
Szerbia	Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	32
	Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	47
	Singidunum Egyetem Belgrád – Informatika Tanszék	63
	Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	59
Az összes hallgatói létszám		**201**

6. táblázat. A kutatásomban részt vett hallgatók eloszolása oktatási intézményenként

6.3 Kutatásban részt vevő hallgatók meglátása a jelenléti ívkészítő rendszer

A jelenléti ív által ellenőrizni lehet a hallgató óralátogatását. Ez szükségszerű, amelyet az oktatók rendszeresen alkalmaznak. Általában a tanórák elején, illetve végén kerül sor a jelenléti ívek kitöltésére. Nagy általánosságban elmondható, hogy a hallgató a tanórák kisebb százalékáról hiányozhat igazolatlanul. Az ezen felüli hiányzást már szankcionálni szokták, úgy, mint az aláírás megtagadást, valamint a tárgyról való letiltást. Ilyen esetben a hallgató nem vehet részt a vizsgán, ez által a tárgy kritériumait sem tudja teljesíteni. Mivel a hallgató ennek a tudatában vannak, ezért igyekszik a tanórákon rendszeresen részt venni.

Az Óbudai Egyetem Hallgatói Követelményrendszerének Tanulmányi és Vizsgaszabályzata szigorúan megköveteli a hallgatóktól a tanórákon való rendszeres részvételt. Ennek ellenőrzése céljából a jelenléti ív alkalmazása szükséges.

Ezen belül a 46. § „Részvétel a foglalkozáson" című fejezet pontosan megfogalmazza az óralátogatással kapcsolatos kritériumokat, amelyeket minden hallgatónak kötelessége betartania. A szabályzat a következő betartandó kritériumokat írja le:

- „Kötelező részt venni a tantermi gyakorlatokon, a laboratóriumi foglalkozásokon, a testnevelési foglalkozásokon, valamint a szakmai gyakorlatokon. Az első éves nappali munkarendű hallgatók számára az előadásokon való részvétel kötelező, továbbá kötelező a levelező munkarendű hallgatók részvétele az órarendi foglalkozásokon. Az előadásokon való részvétel mértékéről az adott tantárgy követelményrendszerében kell rendelkezni.
- A jelenlét ellenőrzésének formáját és a hiányzások igazolásának módját a Tanulmányi Ügyrend tartalmazza.
- Amennyiben a hallgató hiányzásai valamely kötelezően látogatandó tárgyból meghaladják a tárgy félévi összóraszámának 30%-át, a hallgató aláírást, illetve évközi jegyet nem kaphat.
- A hiányzás nem ad felmentést a tantárgyi követelmények teljesítése alól. Mulasztás esetén azok pótlását a hallgató a tantárgyi követelményrendszerben megállapított módon köteles teljesíteni." [103]

Az empirikus kutatásom részeként az online kérdőívem alkalmazása által felmértem azt, hogy a hallgatók hogyan vélekednek a jelenléti ív szükségszerűségéről a tanórák során. A hallgatók többsége az egyetemektől függetlenül (χ^2 próba: p=0,052) igennel felelt arra a kérdésre, miszerint szükség van a jelenléti ívek alkalmazására. Ezt az alábbi hetedik táblázat szemlélteti:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	87%	13%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	76%	24%
Singidunum Egyetem Belgrád – Informatika Tanszék	72%	28%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	71%	29%

7. táblázat. Szerinted szükség van jelenléti ívre a tanórákon? (n=201)

A digitalizáció korában azonban nem csak papíralapú, hanem akár elektronikus jelenléti ívet is lehet készíteni. A kapott válaszok alapján kijelenthető, hogy a hallgatók többsége az egyetemektől függetlenül (χ^2 próba: p=0,059) az elektronikus jelenléti ívet részesítené előnyben a papíralapú megoldással szemben. Mint látható a hallgatók nyitottak az új megoldások iránt. Ezt a következő táblázat bizonyítja:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	51%	49%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	54%	46%
Singidunum Egyetem Belgrád – Informatika Tanszék	57%	43%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	52%	48%

8. táblázat. Meglátásod szerint melyik megoldás lenne a jobb a hallgatói jelenléti ív készítésére? A papír alapú, illetve az elektronikus jelenléti ív? (n=201)

A hallgatói jelenléti ív készítés időigényes feladat, amely a tanórákból értékes perceket képes elrabolni. Célszerű az ilyen rutinszerű feladatokat automatizálni, amely által fontos tanórai időt lehet megtakarítani. Amennyiben a jelenléti ív kitöltésével az oktatóknak nem kellene foglalkozniuk, úgy ezt az időt más fontos teendőkre is fordíthatnák, úgy mint:

- A tanóra eleji ráhangolódás kibővítésére, amellyel a pedagógia széleskörűen foglalkozik,
- A tananyaggal kapcsolatos kérdésekre,
- Több idő maradna a tananyag ismétlésére.

A jelenléti ív nem más, mint információ. Egy olyan hasznos információ, amely az igazolatlan hiányozásokról ad pontos tájokoztatást úgy a hallgatóknak, mint az oktatóknak. A modern oktatás részeként szükségszerű, hogy a hallgatók naprakészen legyenek informálva. A hallgatók arra a kérdésre, hogy szeretnének-e rendszeresen elektronikus értesítéseket kapni a tanórai hiányzásokról a többségük az egyetemektől függetlenül (χ^2 próba: p=0,081) igennel felelt. Ezt a kilencedik táblázat demonstrálja:

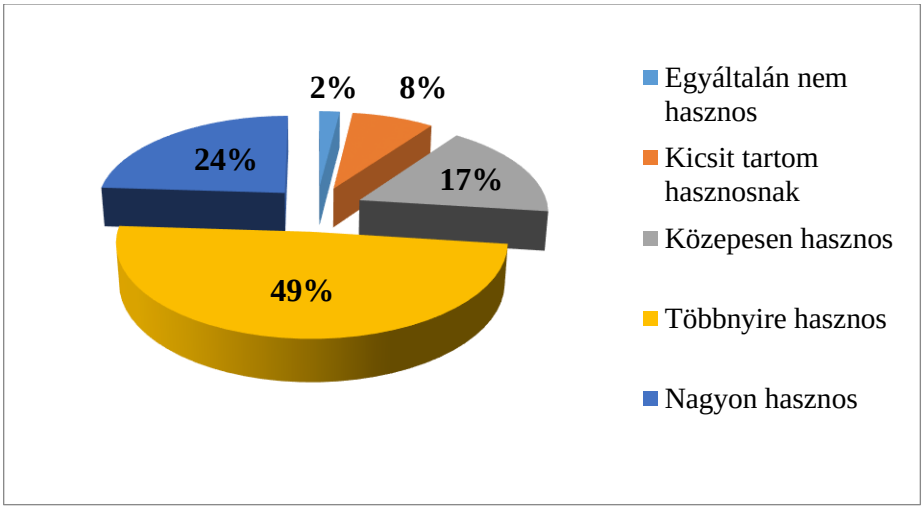
Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	95%	5%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	97%	3%
Singidunum Egyetem Belgrád – Informatika Tanszék	94%	6%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	99%	1%

9. táblázat. Szeretnéd, ha rendszeresen kapnál elektronikus értesítést a tanórai hiányzásaidról? (n=201)

Az elektronikus értesítés előnye:

- Okos eszközökön könnyen megjeleníthető adat,
- A nap bármely részében a jelenléti ívvel kapcsolatos információ a rendelkezésre áll,
- A múltban történt tanórai látogatások könnyen nyomon követhetőek.

Az online kérdőívem segítségével felmértem, hogy a hallgatók hogyan vélekednek egy olyan egyetemi kamerarendszerről, amely alkalmas lehet jelenléti ívkészítésre. A kapott válaszokat az alábbi ábra prezentálja:



14. ábra. Szerinted hasznos lehet az egyetemeken az olyan kamerarendszer, amely hallgatói jelenléti ív készítésére is alkalmas? (n=201)

Mint látható a hallgatók többsége szerint hasznos lehet az egyetemeken az olyan kamerarendszer, amely hallgatói jelenléti ívkészítésére is alkalmas. A szöveges válaszaikból az is kiderült, hogy miért. A hallgatók a következő válaszokat fogalmazták meg:

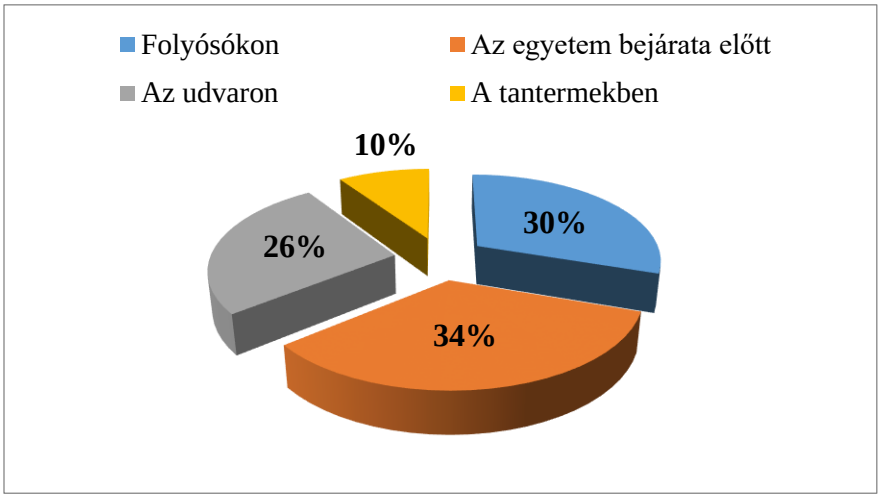
- „Egyszerű és gyors azonosítás”.
- „Nincs szükség arra, hogy a jelenléti ívet egymásak tovább küldjük a tanteremben aláírás céljából”.
- „Nem kell ceruzát keresnem a jelenléti ív kitöltéséhez”.
- „A jelenléti ív kitöltésekor előfordult már, hogy a padtársam olyan nevet is beírt, aki nem volt jelen az órán”.

Mivel a jelenléti ívkészítő rendszer biztonsági kamerákat használ, ezért a hallgatóktól megkérdeztem, hogy szükségesnek tartják-e az egyetemi biztonsági kamerákat? Az egyetemektől függetlenül a többségük erre a kérdésre (χ^2 próba: p=0,055) igennel felelt. Ezt a tizedik táblázat demonstrálja.

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	68%	32%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	71%	29%
Singidunum Egyetem Belgrád – Informatika Tanszék	73%	27%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	77%	23%

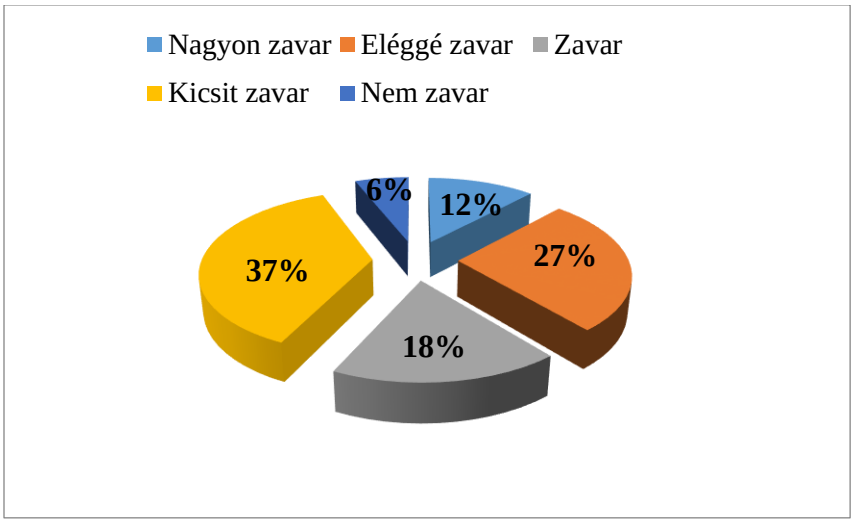
10. táblázat. Szükségesnek tartod az egyetemi biztonsági kamerákat? (n=201)

A következő kérdésemmel azt vizsgáltam, hogy a hallgatók hol látnák legszívesebben ezt a típusú elektronikai védelmi megoldást az oktatási intézményekben? A hallgatók többsége szerint az egyetemek bejárata elé célszerű azokat telepíteni, míg legkevésbé a tantermeket adták válaszul. Ezt a tizenötödik ábra mutatja be:



15. ábra. Szerinted a biztonsági kamerákat hova célszerű elhelyezi a felsőoktatási intézményekben? (n=201)

Tudvalevő, hogy a kamerák képesek a folyamatos megfigyelésre, ezért elképzelhető, hogy a hallgatókat zavarhatja a tantermekben elhelyezett biztonsági kamera. Ezen felül a mesterséges intelligenciával ellátott kamerák akár különböző viselkedési mintákat is képesek felismerni és azokat analizálni. Feltételezhető, hogy a hallgatók ennek tudatában feszélyezve, illetve kellemetlenül érezhetik magukat a tanórákon. Ez extrém esetekben akár a tanórai koncentrációra is képes negatívan kihatni. Hosszabb távon akár a tanulmányi eredményeik is csökkenhetnek. A kutatásom megállapította, hogy a tanulók 57%-át zavarja a tantermi biztonsági kamera. Ezt részletesen a tizenhatodik ábra szemlélteti:



16. ábra. Téged mennyire zavar a tantermekben elhelyezett biztonsági kamera? (n=201)

Az online jelenléti ívkészítésre alkalmas kamerákat elegendő a tantermek bejárata elé elhelyezni, így azok kevésbé zavarják a hallgatókat. Régebben a kamerarendszerek telepítésénél az elsődleges cél kizárólag a kívánt biztonsági szint elérése volt, addig napjainkban a vele járó kényelmetlenség csökkentése, illetve annak teljes megszüntetése is fontos szerepet játszik.

A jelenléti ívkészítésre alkalmas kamerák a beléptetés alkalmával is hasznosak lehetnek. Ilyen esetben az egyetemek bejárata elé kell elhelyezni őket, mivel azok képesek a hallgatókat beléptetéskor regisztrálni, így növelve a biztonsági szintet. Természetesen ez nem azt jelenti, hogy a már jól bevált és működő beléptető-rendszerekre nem lenne szükség. Sőt! A kamerarendszert ajánlatos a beléptető-rendszer mellet kiegészítő biztonsági elemként alkalmazni. A beléptető-rendszerek esetében az azonosítás a következő módokon történhet:

- Tudásalapon. Ez esetben a személy olyan információ birtokában van, amely által beléphet az adott területre. Ennek az információnak az ellenőrzése történik a beléptetés során.
- Birtok alapon. Ilyenkor a személy egy olyan eszköz birtokában van, amely nélkülözhetetlen az azonosítás során. Ez lehet mágneskártya, vonalkód, chipkártya, kulcs.
- Biometria alapon. A személy azonosítása biológiai vagy fizikai jellemzők alapján történik.

A fentebb felsorolt módszereknek léteznek hiányosságaik, ezért a mindennapi életben gyakran két különböző azonosítási módszert együttesen alkalmaznak a kívánt biztonsági szint elérése érdekében. [7] Ezeket az azonosítási típusokat az aktív azonosítási módszerek közé sorolják, mivel a személynek részt kell venniük az azonosításban. A jelenléti ívet használó kamerarendszer alkalmazása által az azonosítás passzív módon történik, mivel ebben az esetben elegendő, hogy a hallgató elhaladjon a kamera előtt.

Amennyiben az egyetem együttesen alkalmazná a birtok- és a biomteria alapú azonosítást kibővítve a jelenléti ív készítésre is alkalmas kamerarendszerrel, úgy egyszerre az aktív és passzív azonosítás is megvalósulhatna. Ez már három különböző azonosítási módszert jelentene, amely feltételezhetően még a legszigorúbb egyetemi beléptetési követelményeknek is eleget tenne. A kamerarendszer kibővítése által a beléptetési idő nem hosszabbodna meg, arra negatívan nem hatna ki.

A jelenléti ívet készítő kamera arcérzékeléssel és arcfelismeréssel rendelkezik, ezen okból kifolyólag a hallgatókat arról kérdeztem, hogy hogyan vélekednek az analitikai kamera funkciókról, szükségesnek tartják-e azokat? A hallgatók többsége az egyetemektől függetlenül (χ^2 próba: p=0,073) erre a kérdésre nemmel felelt. A kapott eredményeket a következő táblázat prezentálja:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	42%	58%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	37%	63%
Singidunum Egyetem Belgrád – Informatika Tanszék	40%	60%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	33%	67%

11. táblázat. Szerinted az arcérzékelésre és felismerésre képes kamera alkalmazására szükség van az egyetem falain belül? (n=201)

A kamera alapú online jelenléti ívkészítésnél fontos szempont kell, hogy legyen a megbízhatóság, a hosszútávú stabil működés és a pontos azonosítás. Ezek együttesen alkotják a bizalmat a kamerarendszer iránt.

A hallgatók meglátása fontos ebben a kérdésben, mivel ők lesznek majd azonosítva napi szinten, az ő adataikat használja a rendszer. Ezen gondolatmenetet követve a hallgatókat arról kérdeztem, hogy szerintük a biztonsági kamerarendszer képes-e őket pontosan azonosítani? A hallgatók többsége az egyetemektől függetlenül (χ^2 próba: p=0,068) igennel felelt erre a kérdésre. A kérdésre kapott válaszokat a tizenkettedik táblázat szemlélteti oktatási intézményenként összegezve:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	61%	39%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	65%	35%
Singidunum Egyetem Belgrád – Informatika Tanszék	58%	42%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	72%	28%

12. táblázat. Szerinted a biztonsági kamera megbízhatóan képes azonosítani a hallgatókat? (n=201)

Ismerve a hallgatói „találékonyságot” még az is elképzelhető, hogy megpróbálják „átvermi” a kamerarendszert az azonosítás során, abból a célból, hogy jogosulatlanul aláírást szerezzenek a jelenléti ívkészítés során. A következő kérdésem ezért azt vizsgálta, hogy a hallgatók hogyan vélekednek az arcfelismerő kamera „kijátszhatóságáról”? A hallgatók meglátása az egyetemektől függetlenül (χ^2 próba: p=0,064), hogy az ilyen kamerákat nehéz „megtéveszteni”. A kapott válaszokat a tizenharmadik táblázat demonstrálja:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	37%	63%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	34%	66%
Singidunum Egyetem Belgrád – Informatika Tanszék	41%	59%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	38%	62%

13. táblázat. Szerinted kijátszható az arcfelismerésre képes biztonsági kamera? (n=201)

7 EMPIRIKUS KUTATÁS II

Az empirikus kutatásom második részében az oktatói véleményeket vizsgáltam a személyazonosításra alkalmas blokklánc alapú jelenléti ívkészítő rendszerről. Erre azért mutatkozott szükség, mivel az oktatók lesznek majd azok a személyek, akik a jelenléti ívkészítő rendszert használni fogják a mindennapok során.

7.1 A kutatásban részt vevő oktatók eloszlása oktatási intézményenként

Az alábbi táblázat a kutatásomban részt vett oktatók eloszlását ábrázolja oktatási intézményenként.

Ország	**Oktatási intézmények**	**Oktatók létszáma**
Szerbia	Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	15
	Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	18
	Singidunum Egyetem Belgrád – Informatika Tanszék	21
	Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	16
Az összes oktatói létszám		**70**

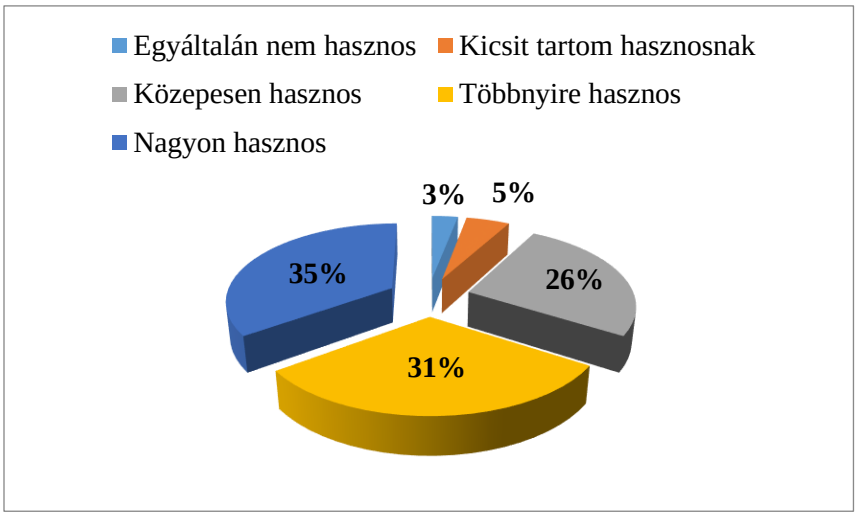
14. táblázat. A kutatásomban részt vett oktatók eloszlása oktatási intézményenként (n=70)

7.2 Kutatásban részt vevő oktatók meglátása a jelenléti ívkészítő rendszerről

A technológia gyors fejlődésének köszönhetően adott a lehetőség arra, hogy az oktatók online jelenléti ívet készítsenek a hallgatóikról.

Az oktatói munkára jellemző, hogy naprakész tananyagokat állítanak elő és tanítanak. Az oktatók folyamatosan követik az új innovációs megoldásokat és lehetőségeket. Mivel ez az életpálya nyitottságot feltételez, ezért elképzelhető, hogy az oktatók szívesen használnának online jelenléti

ívkészítő kamerarendszert. Ezen okból kifolyólag vizsgáltam azt, hogy hogyan vélekednek az automatizált elektronikus kameraalapú jelenléti ív készítésének lehetőségéről, mennyire tartják azt hasznosnak a mindennapok során. A kapott válaszokat a következő ábra mutatja be:



17. ábra. Ön szerint hasznos lehet az oktatási intézményekben egy olyan kamerarendszer, amely hallgatói jelenléti ív készítésére is alkalmas? (n=70) [19]

Megfigyelhető, hogy az oktatók többsége fontosnak tartja a jelenléti ívkészítő megoldást. Szöveges válaszaikban a következőket fogalmazták meg:

- „Érdekes innovatív megoldás”.
- „Tetszik, hogy automatizált módon képes elkészíteni a jelenléti ívet”.
- „Velem már előfordult, hogy a szemeszter során elvesztettem a papíralapú jelenléti ívek egy részét”.
- „Értékes tanórai perceket lehet megtakarítani az alkalmazása által”.
- „Használata által csökkenthető a szükséges papírmennyiség”.
- „Nem kell otthon, illetve az egyetemi szekrényemben tárolni a jelenléti íveket”.

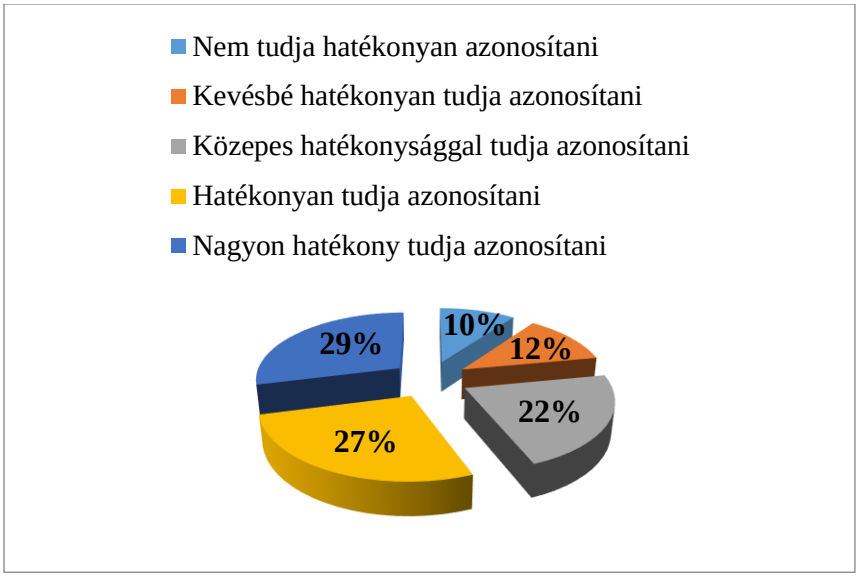
Az elektronikus jelenléti ív jellemzője a folyamatos rendelkezésre állás. Az adatbázisból bármikor lekérhető a hallgatók óralátogatásával kapcsolatos információk. Ezek az adatok a hallgatók számára is a rendelkezésre állnak, azokat meg tudják tekinteni.

Az oktatók arra a kérdésre, hogy fontosnak tartják-e azt, hogy a hallgatók rendszeresen kapjanak értesítést a hiányzásaikról a többségük az egyetemektől függetlenül (p=0,082) igennel felelt. Ez a következő tizenötödik táblázat prezentálja.

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	95%	5%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	96%	4%
Singidunum Egyetem Belgrád – Informatika Tanszék	97%	3%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	94%	6%

15. táblázat. Ön fontosnak tartja, hogy a hallgatók rendszeresen kapjanak elektronikus értesítést a tanórai hiányzásaikról? (n=70)

Mivel a jelenléti ívkészítő kamerarendszer kihasználja az analitikai arcfelismerő funkciókat, ezért az képes felismerni a hallgatókat. Az oktatók meglátása szerint a biztonsági kamerák hatékonyak lehetnek a hallgatók azonosításában. A kapott válaszokat a tizennyolcadik ábra összegzi.



18. ábra. Ön szerint az arcfelismerésre képes kamera hatékonyan tudja azonosítani a hallgatókat? (n=70)

A gyakorlatban bebizonyosodott, hogy a mesterséges intelligenciával rendelkező kamerának idő kell a tanuláshoz. Hatékonysága folyamatosan javul, így a kamera megtanulja kiszűrni azokat az akadályozó tényezőket, amelyek megnehezítik az arcfelismerést.

A kutatásom fontos része, hogy felmérjem az oktatók azon nézőpontját, miszerint lehetőség függvényében használnák-e az online jelenléti ívkészítő rendszert a papíralapú megoldással szemben?

Az oktatók többsége az egyetemektől függetlenül (p=0,075) az előbbi megoldást választaná, amennyiben erre lehetőségük adódna. A válaszok összegzését az alábbi tizenhatodik táblázat mutatja be.

Egyetemek	**Automatizált elektronikus jelenléti ívkészitő rendszer**	**Papíralapú jelenléti ív**
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	54%	46%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	65%	35%
Singidunum Egyetem Belgrád – Informatika Tanszék	63%	37%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	69%	31%

16. táblázat. Amennyiben adott lenne a lehetőség, Ön a kamerarendszeren alapúló hallgatói jelenléti ívkészítő rendszert használná a mindennapokban, illetve a papíralapú megoldást választaná? (n=70) [19]

Az empirikus kutatásom részeként célszerű volt a jelenléti ívek szükségességét az oktatók szempontjából is megvizsgálni. A kapott eredmények alapján kijelenthető, hogy jelentős többségük az egyetemektől függetlenül (p=0,055) fontosnak tartja a kérdőívek alkalmazását. Ezt a tizenhetedik táblázat szemlélteti:

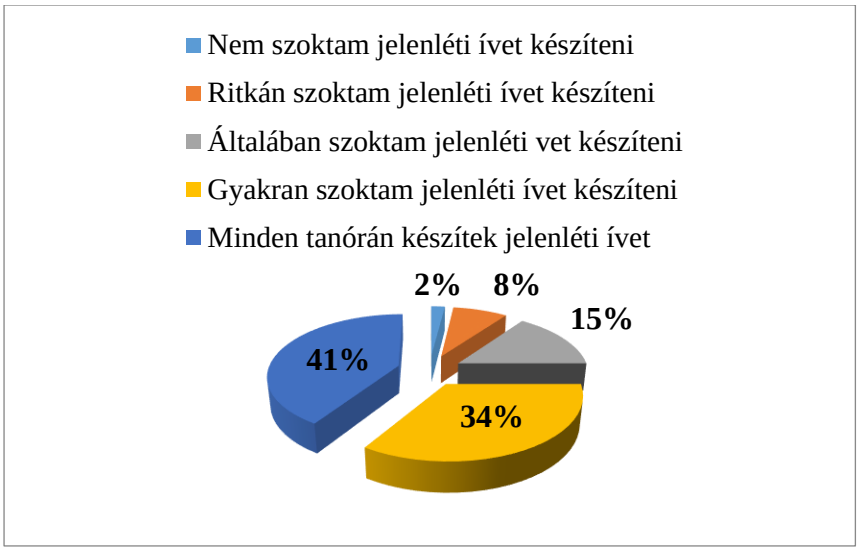
Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	92%	8%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	94%	6%
Singidunum Egyetem Belgrád – Informatika Tanszék	95%	5%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	93%	7%

17. táblázat. Ön szerint szükség van jelenléti ívre a tanórákon? (n=70)

Ennek fontosságáról a következő válaszokat fogalmazták meg:

- „Jelenléti ív alkalmazása nélkül a hallgatók nem látogatják rendszeresen a tanórákat”.
- „A hallgatók mivel rendszeresen részt vesznek a tanórákon, jobban megértik a tananyagokat”.
- „Jobb érdemjegyeket szereznek a tanulók, mivel a tanórák többségén részt vesznek, ez által eredményesebb vizsgát tesznek”.

Továbbá feltérképeztem azt is, hogy az oktatók milyen gyakran készítenek jelenléti ívet. Ez azért lényeges információ, mivel ez a kérdés a kérdőívek alkalmazásának szükségességére mutat rá, illetve annak gyakori használatát tárja fel. A kapott eredményeket a tizenkilencedik ábra demonstrálja:

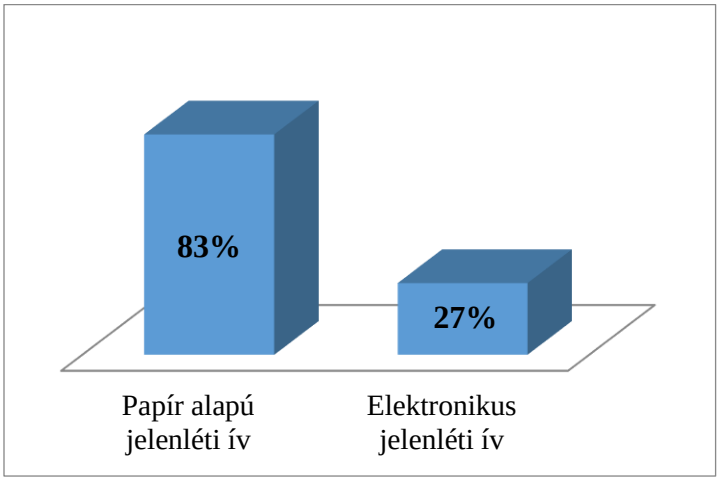


19. ábra. Ön milyen gyakorisággal készít hallgatói jelenléti ívet a tanórákon? (n=70)

Megállapítottam, hogy az oktatók 75%-a, azaz jelentős többségük, ha nem is minden tanórán, de gyakran használ jelenléti ívet.

Tudvalevő, hogy a jelenléti ívek többféle képen is elkészíthetőek. A papír alapú jelenléti ív több évszázados múltra tekint vissza, míg az elektronikus jelenléti ív újdonságnak számít. Észrevehető, hogy az egyetemi jelenléti ív szorosan kapcsolódik az oktatáshoz, annak fontos elemét képezi.

Az oktatók arra a kérdésre, hogy a papír, illetve az elektronikus jelenléti ívet használnak-e a tanórákon a következő válaszokat adták, amelyet az alábbi ábra prezentálja.



20. ábra. Ön papíralapú, illetve elektronikus jelenléti ívet használ a tanórákon? (n=70)

Megállapítottam, hogy az oktatók a papíralapú megoldást részesítik előnyben, mivel azokat használják a leggyakrabban. Szöveges válaszaikban a következő magyarázatokat fogalmazták meg:

- „A papíralapú jelenléti ív használatát már megszoktam a mindennapok során."
- „Könnyen elboldogulok a papíralapú jelenléti ívvel."
- „Egyszerű a papíralapú jelenléti ív használata, nem igényel számítógépet."
- „Nincsen rendelkezésre álló elektronikus jelenléti ív."

Az online jelenléti ívkészítő kamerarendszer használata nem bonyolult feladat, mivel számos teendőt automatizáltan lát el. Mint minden technikai berendezés használatához, ehhez sem árt egy bizonyos szintű alaptudás. Az oktatók többsége nyitott az ismeretszerzés ezen területén, mivel a többségük az egyetemektől függetlenül (χ^2 próba: p=0,073) szívesen megtanulná a rendszert használni. Szükség esetén akár ez irányú képzésben is részt vennének. A válaszokat az alábbi táblázat mutatja be:

Egyetemek	Igen	Nem
Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar, Szabadka	52%	48%
Óvó- és Edzőképző Szakirányú Főiskola, Szabadka	57%	43%
Singidunum Egyetem Belgrád – Informatika Tanszék	54%	46%
Singidunum Egyetem Belgrád – Közgazdaságtan Tanszék	53%	47%

18. táblázat. Ön egy önkéntes képzés keretében megtanulná használni a jelenléti ívkészítésre alkalmas kamerarendszert? (n=70)

ÖSSZEGZETT KÖVETKEZTETÉSEK

A doktori tanulmányomat 2017-ben kezdtem. A tanulmányom során számos tudományos munkát megjelentettem a kutatási témámmal kapcsolatban, úgy hazai, mint külföldi folyóiratokban és konferenciákon. A kutatásom alatt a tudományos eredményeimet folyamatosan publikáltam.

A kutatási témám a „Személyazonosításra alkalmas automatizált elektronikus blokklánc kialakítása” volt. Négy évig kutattam és vizsgáltam annak az lehetőségét, hogy az iskolai biztonsági kamerák tudását, hogyan lehetne kibővíteni úgy, hogy az az oktatási intézmények számára új lehetőséget biztosítson.

Megállapítottam ahhoz, hogy a biztonsági kamerákát alkalmazni lehessen a jelenléti ívkészítés során a következő analitikai funkciókkal kell, hogy rendelkezzenek, úgy, mint arcérzékelés, arcazonosítás, létszám megállapítás, arcadatbázis és mesterséges intelligencia. A kamerák által generált adatmennyiségek csökkentése érdekében megvizsgáltam a rendelkezésre álló videó tömörítési eljárásokat és arra a megállapításra jutottam, hogy a H.265 típusú videó tömörítő algoritmus alkalmazása biztosítja a leghatékonyabb adat tömörítést, ezért a gyakorlati megvalósításom során ezt a tömörítési megoldást választottam.

Mivel a centralizált adattárolási megoldások nem nyújtanak kellő biztonságot, ezért részleteiben megvizsgáltam a nyilvános és a privát blokklánc technológiában rejlő lehetőségeket. Megállapítottam, hogy a privát blokklánc technológia alkalmazása által növelni tudom az adatbázis-biztonságot, ezért létrehoztam egy saját ÓUDSC nevű blokkláncot, ahova érzékeny hallgatói adatokat mentettem el. A blokklánc létrehozása során meghatároztam az optimális blokkméret nagyságot, amely 1MB volt. Erre azért volt szükség, hogy a blokklánc gyors legyen. Ennél nagyobb blokkméret értelemszerűen lassabb blokklánc működést eredményezett volna.

Megállapítottam, hogy a genezis blokk létrehozása után a blokkláncot össze lehet kapcsolni az NVR egységgel. E célból okos szerződést használtam, valamint rögzítettem a szerződési feltételeket. Ennek eredményeként a videófelvételek küldése a blokklánc adatbázisába automatizált módon végrehatódott. Abból a célból, hogy a hallgatói adatok a küldés során ne kompromitálódjanak azokat ujjnyomatokkal láttam el. Ennek megvalósítását a biztonsági kamerarendszer és a blokklánc közötti kapcsolat modellel prezentáltam, valamint a biztonság

további fokozása érdekében az adatokat időbélyeggel láttam el az SHA 512-es titkosítási eljárás alkalmazása mellett.

A kutatásomban rávilágítottam arra is, hogy az ÓUDSC blokklánc alapú jelenléti ívkészítő kamerarendszer a tűzvédelemben is alkalmazható. A már meglévő tudása hozzájárult ahhoz, hogy azt alkalmazni lehessen az oktatási intézményekben. Megállapítottam, hogy a kamerarendszer számos módon segítheti a mentőalakulatok dolgát, úgy, mint a tűzoltók kiérkezésekor azonnal információt nyújt a hallgatók tartózkodási helyéről, valamint tűz esetén riasztja az előerős védelmet.

Bebizonyítottam, hogy a biztonsági kamerák által létre lehet hozni egy automatizált elektronikus online jelenléti ívkészítő rendszert. Az empirikus kutatásom részeként megállapítottam, hogy a felsőoktatásban dolgozó oktatók szívesen alkalmaznának egy ilyen megoldást a mindennapok során, valamint azt is, hogy a hallgatókat nem zavarja a biztonsági kamerákon alapuló jelenléti ívkészítő rendszer a tantermek bejárata előtt.

A Biztonságtudományi Doktori Iskola hallgatójaként mindvégig fontos szempont volt, hogy a hallgatói jelenléti ívkészítő rendszer az adatok tárolását biztonságosan oldja meg. Ezért olyan új technológiai megoldást kellett megismernem, majd pedig alkalmaznom, amellyel még jelenleg is ismerkedik a tudományos világ. Ez a blokklánc technológia.

Remélem, hogy a befektetett energia és szorgalom által egy olyan tudományos módszereken alapuló disszertációt sikerült megalkotnom, amely méltán képes az Óbudai Egyetem Biztonságtudományi Doktori Iskola jóhírét öregbíteni.

Összefoglalva a munkámat befejeztem, azt lezártnak tekintem.

„Ha egy tudomány problémára bukkan, azt csak a tudás oldhatja meg.”

Isaac Asimov [104]

Hipotézisek igazolása, elvetése

A hipotézisek vizsgálata során a legjobb tudásom szerinti pontosságra törekedtem. A disszertációmban öt fő hipotézist fogalmaztam meg. Ezek a hipotézisek igazolást nyertek.

Első lépésként megvizsgáltam, hogy adottak-e azok feltételek, amelyek által létre lehet hozni egy olyan személyazonosításra alkalmas automatizált elektronikus hallgatói jelenléti ívkészítő rendszert, amely biztonsági kamerákat, blokklánc technológiát és okos szerződést is alkalmaz? A már rendelkezésre álló tudományos munkák és műszaki eszközök áttekintése után a tervezett rendszert megvalósítottam, így a hipotézisem igazolást nyert. Mivel az ÓUDSC blokklánc által az adatok ujjnyomattal is elláthatóak, így bebizonyosodott, hogy az adatok biztonságosan tárolhatóak, azok kevésbé érzékenyek a manipulációval szemben. Mivel a rendszer képes a hallgatók nyomon követesére, így azt a tűzvédelemben is alkalmazni lehet.

Induktív kutatást alkalmazva online kérdőív segítségével a felsőoktatásban dolgozó oktatók és hallgatók meglátását feltártam a jelenléti ívkészítő rendszerrel kapcsolatban. Bebizonyosodott, hogy az oktatók és a hallgatók is hasznos megoldásnak találják a személyazonosításra alkalmas blokklánc alapú jelenléti ívkészítő rendszert.

A hipotéziseimet alátámasztottam, mivel a rendszer megvalósult, valamint annak hasznosságát is ellenőriztem empíria által.

Új tudományos eredmények

A kutatásom során egy olyan automatizált hallgatói jelenléti ívkészítő rendszert dolgoztam ki, amelyet az oktatási intézmények akár a mindennapok során is használhatnak. Ennek részeként öt fő tézist fogalmaztam meg, amelyek szorosan kapcsolódnak a célkitűzésekhez és a kutatási kérdésekhez. A megfogalmazott hipotéziseim bebizonyosodtak, ezért kijelenthető, hogy újszerű tudományos eredmények születtek. Ezt az alábbi táblázat prezentálja.

Téziscsoport	
T1.	A biztonsági kamerák analitikai funkcióinak vizsgálatát követően bebizonyítottam, hogy a rendszer képes felismerni és azonosítani a hallgatókat. A blokklánc technológia elemzése után létrehoztam egy saját ÓUDSC nevű egyetemi blokkláncot, amelyet okos szerződés segítségével összekapcsoltam, így a hallgatók adatai automatizált módon kerültek mentésre a blokkláncba. A rendszer gyakorlati megvalósítása igazolta a hipotézist.
T2.	A jelenléti ívkészítő rendszer funkcióinak vizsgálata során bebizonyítottam, hogy a rendszer képes a hallgatók arcképeihez időbélyeget rendelni, ez által bizonyítva, hogy a hallgató arcképe az adott időpontban azonosításra került így csökkentve a visszaélések lehetőségét.
T3.	Igazoltam, hogy a jelenléti ívkészítő rendszer képes a hallgatók tartózkodási helyét azonosítani és nyomon követni, ezért kijelenthető, hogy a rendszer az elektronikai tűzvédelem részét képezheti.
T4.	A kutatás eredményeivel bizonyítottam, hogy a személyazonosításra alkalmas jelenléti ívkészítő kamerarendszer nem okoz hallgatói frusztrációt, valamint kellemetlenséget. Az empirikus kutatás alapján igazoltam, hogy a hallgatók előnyben részesítik a digitális jelenléti ívet a papíralapú megoldással szemben.
T5.	Az empirikus kutatásaimmal bebizonyítottam, hogy az egyetemi oktatók a gyakorlati megvalósítás során hasznos megoldásnak találták a személyazonosításra alkalmas elektronikus blokklánc alapú jelenléti ívkészítő rendszert, mivel szívesen alkalmazták a tanóráikon.

19. táblázat. Téziscsoportok

Ajánlások és a kutatási eredmények hasznosítása

A kutatási eredményeimet a műszaki tudományok területén lehet hasznosítani, mivel az alábbi kutatási eredmények kerültek megvalósításra:

- Automatizált elektronikus jelenléti ívkészítő rendszer kidolgozása,
- Egyetemi blokklánc létrehozása adattárolás céljából,
- Modern elektronikai tűzvédelmi megoldás kidolgozása biztonsági kamerarendszerek alkalmazása által,
- Okos szerződés segítségével a blokklánc összekapcsolása az NVR egységgel.

A kutatási eredményeimet nem csak az oktatási rendszerben lehetne felhasználni, hanem a katonai műszaki tudományok területén is. A kapott kutatási eredmények olyan technológiai és műszaki innovációs jellegűek, amelyeket akár az objektumvédelemben, valamint a speciális objektumvédelemben is kamatoztathatóak. [10]

Ezek a következők:

- Kórházak biztonsága, ahol a betegek és az ott dolgozók biztonságát lehetne növelni, mivel a rendszer képes az épületben tartózkodók folyamatos nyomon követesére és azonosítására.
- Modern betegazonosítás, mint új vagyonvédelmi rendszer kialakítása. Az elmúlt években nem egy esetben előfordult, hogy a műtétek során téves betegazonosításra került sor. [11] A jelenléti ívkészítő rendszer és annak blokklánc adatbázisa ebben nyújthat segítséget. A beteg személyazonossága mellett a blokkláncban biztonságosan tárolhatók a betegséghez kapcsolódó adatok. A műtőben való belépéskor a rendszer képes azonosítani a beteget, valamint annak betegségét is megjelenítheti a kijelzőn.
- Veszélyes anyagokat vizsgáló laboratóriumok esetében, mivel a rendszer képes nyomon követni az alkalmazottak tartózkodási helyét. Amennyiben valaki illetéktelen területre tévedne, úgy jogosultság hiányában a rendszer riaszthatná az élőerős védelmet. A speciális objektumvédelem esetében még inkább fontos az adatok biztonságos tárolása. A kamerarendszer az adatokat ebben az esetben egy privát blokkláncban tárolná el.

A kutatás távlatai, nyitott kérdések

A disszertációhoz kapcsolódó kutatás lezárultával a jövőben további fejlesztési útvonalakat szükségszerű meghatározni, abból a célból, hogy az automatizált blokklánc alapú hallgatói jelenléti ívkészítő rendszer piaci bevezetése megtörténhessen, azt az oktatási intézmények megvásárolhassák.

- Célszerű lenne több biztonsági kamerát is megvizsgálni, abból a célból, hogy az értékesítés során több jelenléti ívkészítő rendszer csomagot lehessen kínálni az oktatási intézmények számára.
- A rendszer hatékonyabb telepítése érdekében az Off-Chain blokklánc technológia további kutatása szükséges.
- Egy átlátható felhasználói felület kidolgozása szükségszerű.
- Használati útmutató készítése a jelenléti ívkészítő rendszer szakszerű alkalmazásáról.

Nyitott kérdésként fogalmazódik meg a blokklánc használatának törvényi szabályozásának vizsgálata, annak alkalmazása adattárolás céljából. Jelenleg a blokklánc technológia nincsen kellőképpen szabályozva, annak elfogadottsága országonként változhat.

IRODALOMJEGYZÉK

[1] BEREK Lajos - BEREK Tamás - BEREK László.: Személy és vagyonbiztonság, ÓE-BGK 3071, Budapest, 2016. https://bit.ly/3t1pfDH (letöltve: 2022.07.21.)

[2] BÁLINT Krisztián.: Possibilities of the Application of Solar Powered Security Systems at the Universities of Subotica, Serbia; 2018 International IEEE Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), New York (NY), Amerikai Egyesült Államok, Piscataway (NJ), pp. 277-282, 6 p. 2018. https://bit.ly/3IuTnkc (letöltve: 2022.07.21.)

[3] BÁLINT Krisztián.: Modern, Decentralized Blockchain-Based Solutions for Saving Video Footage; IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY 2020) Danvers (MA), Amerikai Egyesült Államok: IEEE, 185 p. pp. 11-14, 4 p. 2020. https://bit.ly/3eDB7X7 (letöltve: 2022.07.21.)

[4] TOKODY Dániel.: Doktori értekezés: Intelligens vasúti informatikai és biztonsági rendszerek fejlesztése; Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2020. https://bit.ly/3gO1ZGL (letöltve: 2022.07.21.)

[5] TOKODY Dániel - SCHUSTER György-PAPP József: Study of how to implement an intelligent railway system in Hungary; Intelligent Systems and Informatics (SISY), IEEE 13th International Symposium, 2015. https://bit.ly/3dWgnuT (letöltve: 2022.07.21.)

[6] DEZSŐ András.: A szemünk előtt épült ki a digitális diktatúra; 2018. https://bit.ly/392zwpW (letöltve: 2022.07.21.)

[7] BÁLINT Krisztián.: Connecting Bitcoin Blockchain with Digital Learning Chain Structure in Education; Acta Polytechnica Hungarica, Volume 16, Issue Number 1, 2019. https://bit.ly/3gND7yP (letöltve: 2022.07.21.)

[8] CATHY Sturges.: Cointelegraph - How Can Blcokchain Improve Date Storage; 2019. https://bit.ly/3gND7yP (letöltve: 2022.07.21.)

[9] PRINCE Waqas Khan – YUN - Cheol Byun - NAMJE Park.: A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities; MDPI Journal Electronics, 2020. https://bit.ly/3xv4cfZ (letöltve: 2022.07.21.)

[10] CEDENO Jesús.: How Blockchain Could Impact Education in 2020 and Beyond; GETTING Smart, 2020. https://bit.ly/3jo7utd (letöltve: 2022.07.21.)

[11] MAUREEN Hance.: What is Blockchain and How Can it be Used in Education; 2020. https://bit.ly/34pffea (letöltve: 2022.07.21.)

[12] ANDRÉ Vitalin.: Kamerás megfigyelés, biztonság és szabadságjogok; Információs Társadalom 2.1, 2002. https://bit.ly/3vtuLAF (letöltve: 2022.07.21.)

[13] BARA Norbert.: Automatikus videó megfigyelő rendszer; Diplomadolgozat, Szegedi Tudományegyetem Informatikai Tanszékcsoport, 2006. https://bit.ly/3ew3Wou (letöltve: 2022.07.21.)

[14] RICK Delgado.: From Edison to Internet: A History of Video Surveillance; 2013. https://bit.ly/3fkG59R (letöltve: 2022.07.21.)

[15] OKTEL Elektronika.: A CCTV története; 2018. https://bit.ly/2PgxwC9 (letöltve: 2022.07.21.)

[16] BÁLINT Krisztián.: Iskolai biztonság fontosága; Berek Hetven: Egy élet a hadtudomány és a művészet szolgálatában, a hetvenéves Berek Lajos professzor és szobrászművész köszöntése; Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, ISBN:9789634491576, pp. 33-42, 10 p. 2019. https://bit.ly/3RYtQEq (letöltve: 2022.07.21.)

[17] ALPHASONIC.: Hogyan nő a videónalalitika értéke; 2018. https://bit.ly/3ageeXf (letöltve: 2022.07.21.)

[18] SURVEILLANCE - Privacy – Security.: Megfigyelés, magánszfére és biztonság;Az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramjának készült felmérés, 2020. https://bit.ly/33KTlSZ (letöltve: 2022.07.21.)

[19] LIEBMANN Gábor.: Alapvető hasonlúságok és különbségek az analóg és az IP kamerarendszerek között; XII. Évfolyam 3. szám. szeptember, 2017. https://bit.ly/3aO4AQx (letöltve: 2022.07.21.)

[20] CSURGA Design.: Mi az a JPEG; 2011. https://bit.ly/3gt41Jw (letöltve: 2022.07.21.)

[21] OKTEL Elektronika.: A képtömörítés; 2018. https://bit.ly/3fmMaTa (letöltve: 2022.07.21.)

[22] ONSSI Systems.: MJPEG vs MPEG4, Understanding the differences, advantages and disadvantages of each compression technique; 2006. https://bit.ly/3B4dOmo (letöltve: 2022.07.21.)

[23] FORGÓ Sándor.: Tömörítési szabványok; 2015. https://bit.ly/3fn6Ni4 (letöltve: 2022.07.21.)

[24] HARILAOS Koumaras - MICHAIL Alexandros Kourtis, DRAKOULIS Martakos.: Benchmarking the Encoding Efficiency of H.265/HEVC and H.264/AVC; ICT Future Network and MobileSummit 2012, Estrel Berlin, Germany, 04 - 06 July, 2012. https://bit.ly/3sXujcj (letöltve: 2022.07.21.)

[25] LACKÓ Gábor.: Mi az a H.264 tömörítési technológia; Computerworld, 2008. https://bit.ly/3dyfMwO (letöltve: 2022.07.21.)

[26] ERDŐS Márton.: Sok a kérdés az új tömörítés körül; 2016. https://bit.ly/3cxDGXJ (letöltve: 2022.07.21.)

[27] BÁLINT Krisztián.: Composition of an Automated Attendance Register of Students by Security Cameras, as Part of Smart City; Interdisciplinary Description of Complex Systems, Budapest, Óbudai University, Smart City, pp. 27-36, 10p. 2016. https://bit.ly/3nUPXgX (letöltve: 2022.07.21.)

[28] BÁLINT Krisztián.: Biztonsági kamerákon alapuló hallgatói jelenléti ívkészítő rendszer analitikai funkciói; Rendészet-Tudomány-Aktualitások, A rendészettudomány a fiatal kutatók szemével, Doktoranduszok Országos Szövetsége Rendészettudományi Osztály Budapest, pp. 42-49, 8 p. 2021. https://bit.ly/3ADXZCG (letöltve: 2022.07.21.)

[29] BÁLINT Krisztián.: Biztonsági kamerákon és blokklánc technológián alapuló hallgatói jelenléti ívkészítő rendszer működésének modellje és annak felépítése; XXIV. Tavaszi Szél Konferencia 2021, Budapest, Magyarország: Doktoranduszok Országos Szövetsége (DOSZ) 667 p. pp. 217-217, 1 p. 2021. https://bit.ly/3oeSeUD (letöltve: 2022.07.21.)

[30] CHENGBIN Peng - WEI Bu - JIANGJIAN Xiao - KACHUN Wong - MINMIN Yang.: An Improved Neural Network Cascade for Face Detection in Large Scene Surveillance; Journal Applied Sciences, 2018. https://bit.ly/3dYfDFe (letöltve: 2022.07.21.)

[31] MARION Gentele - ALEXANDER Lewinksy.: Jobb biztosra menni! Arcdetektálás az UI-3013XC kamerával; 2015. https://bit.ly/37neqkw (letöltve: 2022.07.21.)

[32] SZŰCS Gábor - SALLAI Gyula.: Az okos város kameraképeinek elemzése, Budapest, Dialog Campus Kiadó, 2019. https://bit.ly/3aILcRD (letöltve: 2022.07.21.)

[33] ARISTEIDIS Tsitiridis - CRISTINA Conde - BEATRIZ Gomez Ayllon - ENRIQUE Cabello.: Bio-Inspired Presentation Attack Detection for Face Biometrics; Fronteiers in Computational Neuroscience, Volume 13, Article 34, 2019. https://bit.ly/3sZb2ah (letöltve: 2022.07.21.)

[34] SOOYEON Kim - YUSEOK Ban - SANGYOUN Lee.: Face Liveness Detection Using Defocus; Sensors Journal, 2015. https://bit.ly/2PqHkx6 (letöltve: 2022.07.21.)

[35] MARK Andrejevic-NEIL Selwyn: Facial recognition technology in schools, critical questions and concerns, Learning. Media and Technology, 2019. https://bit.ly/3gMCghQ (letöltve: 2022.07.21.)

[36] SECURIFOCUS.: Dual-lens emberszámláló kamera - Hikvision iDS-2CD6810F-IV/C; 2019. https://bit.ly/2AoOlHl (letöltve: 2022.07.21.)

[37] FINJAN Team.: Blacklisting vs Whitelisting – Understanding the Security Benefits of Each; 2017. https://bit.ly/2UKDQFp (letöltve: 2022.07.21.)

[38] FAZEKAS Attila - SZEGHALMY Szilvia - BARTÓK Kornél - SAJÓ Levente.: Multimodális ember-gép kapcsolatok; Debreceni Egyetem, Debreceni Képfeldolgozó Csoport, 2011. https://bit.ly/3sR3PJm (letöltve: 2022.07.21.)

[39] JIANHUA Zhanga - ZHONG Yinb - PENG Chenc - STEFANO Nichele.: Emotion recognition using multi-modal data and machine learning techniques; A tutorial and review, Information Fusion, Elseiver Journal, 2020. https://bit.ly/2QHJokT (letöltve: 2022.07.21.)

[40] NÉMETH Gábor.: Arcdetektálás és -felismerés beltéri videófolyamokban; Szegedi Tudományegyetem, 2015. http://bit.ly/34kFBeg (letöltve: 2022.07.21.)

[41] MÉRNÖKI Szolgáltató, Hogyan működik a hőkamera; 2019. https://bit.ly/3fu0F7J (letöltve: 2022.07.21.)

[42] AMBRUS Éva.: Blokkláncok; Hadmérnök, XII évfolyam, 2. szám, június, 2017. https://bit.ly/3nvWGNE (letöltve: 2022.07.21.)

[43] AZARIA Asaph.: Medrec: Using blockchain for medical data access and permission management; 2nd International Conference on Open and Big Data (OBD). IEEE, 2016. https://bit.ly/3gKHxGU (letöltve: 2022.07.21.)

[44] ZIBIN Zheng - SHAOAN Xie - HONG Ning Dai - XIANGPING Chen - HUAIMIN Wang.: Blockchain challenges and opportunities: a survey; International Journal of Web and Grid Services, 14(4), 352-375. 2018. https://bit.ly/3yUIPGx (letöltve: 2022.07.21.)

[45] TANZEELA Sultana - AHMAD Almogren - MARIAM Akbar - MANSOUR Zuair - IBRAR Ullah - NADEEM Javaid.: Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices; Applied Sciences 10.2, 488, 2020. https://bit.ly/3t0HAkd (letöltve: 2022.07.21.)

[46] LUKA Müller - Thomas Linder.: Public vs Private Ledger; 2019. https://bit.ly/3fRgEgk (letöltve: 2022.07.21.)

[47] TIEN Tuan Anh Dinh - MEIHUI Zhang - GANG Chen.: Untangling Blockchain: A Data Processing View of Blockchain Systems; IEEE Transactions on Knowledge and Data Engineering 30.7, 1366-1385. 2018. https://bit.ly/3vqGS18 (letöltve: 2022.07.21.)

[48] COINMIXED.: Mi a különbség a publikus, privát és az engedélyköteles blokkláncok között; 2021. https://bit.ly/3vqGS18 (letöltve: 2022.07.21.)

[49] ANTAL Molnár Nikolett.: A kriptovalutától a digitális valutáig; Konferenciakötet, Válogatott tanulmányok, Pécs. 141 p. pp. 4-14, 11 p. 2022. https://bit.ly/3PplTpU (letöltve: 2020.02.27.)

[50] BITCOINBÁZIS.: Mire jók a privát blokkláncok; 2018. https://bit.ly/2ArxN0T (letöltve: 2022.07.21.)

[51] BÁLINT Krisztián.: Modern, Blockchain-Based Fire Protection Solutions Through In-School Security Cameras; Hadmérnök, Volume Number: 15, Issue: 4, Pages: 5-14. 2020. https://bit.ly/3sW7u8Q (letöltve: 2022.07.21.)

[52] ARAN Devies.: Public vs Private (Permissioned) Blockchain Comparison; 2021. https://bit.ly/30T2gQm (letöltve: 2022.07.21.)

[53] PRAVEEN Jayachandran.: The difference between public and private blockchain; 2017. https://ibm.co/3gSHciq (letöltve: 2022.07.21.)

[54] BINANCE.: Private, Public and Constortium Blockchains, What's the Difference; 2020. https://bit.ly/2PPevHi (letöltve: 2022.07.21.)

[55] BUDAI Gergő.: Blockchain a kriptovaluták és az okos szerződések világa; Budapesti Gazdasági Egyetem, Gazdálkodási Kar, Zalaegerszeg, 2018. https://bit.ly/3vw0TDP (letöltve: 2022.07.21.)

[56] VIRTUÁLIS Cash.: Mi az okos szerződés; 2020. https://bit.ly/2BgOUn5 (letöltve: 2022.07.21.)

[57] KÖRNYEI Mátyás.: Programozott kollektív bölcsesség – Az okos szerződések alapkérdései; 2018. https://bit.ly/2CxR1n3 (letöltve: 2022.07.21.)

[58] STEFÁN Ibolya.: Az okos szerződések létrejöttének és érvénytelenségének kérdései; Miskolci Jogi Szemle 16.3, 298-312. 2021. https://bit.ly/3v4Q9yd (letöltve: 2022.07.21.)

[59] HONTI Roland.: CRYPTO Falka, Mi is az az okos szerződés, avagy smart contract; 2020. https://bit.ly/2OGFMv0 (letöltve: 2022.07.21.)

[60] BÁLINT Krisztián.: Lehetséges modern információbiztonsági megoldások az iskolai biztonsági kamerarendszerek tároló architektúráját illetően; Kiberbiztonság - Cyber Security: Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból, Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, pp. 141-153., 12 p. 2018. https://bit.ly/3xv9U1D (letöltve: 2022.07.21.)

[61] HÍRMAGAZIN.: DAS, NAS, SAN - or storages on the network; 2004. https://goo.gl/DdcyZ5 (letöltve: 2022.07.21.)

[62] SIMA Dezső - SCHUBERT Tamás.: Data centers; Óbudai University, John von Neumann Faculity of Informatics, 2011. https://bit.ly/3OmohfO (letöltve: 2022.07.21.)

[63] IPON.: Micsoda és mire jó egy NAS; 2017. https://bit.ly/2LWj28Y (letöltve: 2022.07.21.)

[64] ELTE.: SAN hálózatok – Az adattároló hálózatok fejlődése; 2018. https://goo.gl/gCgRSL (letöltve: 2022.07.21.)

[65] AREA Network.: Fibre Channel; 2016. https://goo.gl/M179L1 (letöltve: 2022.07.21.)

[66] PAPP Gábor.: Raid kötet egyszerűen I; 2007. https://goo.gl/D3881j (letöltve: 2022.07.21.)

[67] ERDŐS Márton.: Így működik a RAID. 2014. https://goo.gl/srSu9F (letöltve: 2022.07.21.)

[68] UNIX Linux.: Diskless vékonykliensek bootolása iSCSI targetről, konfiguráció; 2009. https://bit.ly/3abAv7T (letöltve: 2022.07.21.)

[69] HUIGE Li - FANGGUO Zhang - PEIRAN Luo1 - HAIBO Tian1 - JIEJIE He.: How to retrieve the encrypted data on theblockchain; KSII Transactions on Internet and Information Systems vol. 13, no. 11, Nov. 2019. https://bit.ly/3aL11qQ (letöltve: 2022.07.21.)

[70] ANDREW Tar.: Decentralized and Distributed Databases Explained; 2017. https://bit.ly/2ZEBqtl (letöltve: 2022.07.21.)

[71] PENG Jiang - FUCHUN Guo - KAITAI Liang - JIANCHANG Laib - QIAOYAN Wen.: Searchain: Blockchain-based Private Keyword Search in Decentralized Storage; Elseiver 2017. https://bit.ly/3aNrIeK (letöltve: 2022.07.21.)

[72] AMER Rosic.: Centralized vs Decentralized Storage, Redefining Storage Solutions with Blockchain; 2020. https://bit.ly/2NxIrX9 (letöltve: 2022.07.21.)

[73] PARIKSHIT Hooda.: Comparison – Centralized, Decentralized and Distributed Systems. 2021. https://bit.ly/3dYwLYw (letöltve: 2022.07.21.)

[74] BÁLINT Krisztián.: Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a Universities' Modern Security Cameras; Acta Polytechnica Hungarica, DOI: 10.12700/APH.18.2.2021.2.7, Volume 18, Issue Number 2, 2021. https://bit.ly/3IQgLZH (letöltve: 2022.07.21.)

[75] CRYPTOCURRENCY Statistics.: Különböző coin típusoknak a blokklánc méretei; 2022. https://bit.ly/3ueCzX1 (letöltve: 2022.07.21.)

[76] BÁLINT Krisztián.: Modern, Decentralized Blockchain-Based Solutions for Saving Video Footage; IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY

2020) Danvers (MA), Amerikai Egyesült Államok: IEEE, 185 p. pp. 11-14, 4 p. 2020. https://bit.ly/3PmBuGT (letöltve: 2022.07.21.)

[77] ALEX van de Sande.: Ethereum blog, How to build serverless applications; 2016. https://bit.ly/3fBjLJO (letöltve: 2022.07.21.)

[78] GÁBOR Tamás - KISS Gábor Dávid.: Bevezetés a kriptovaluták világába; Gazdaság és Pénzügy, 1. Szám, 5. Évfolyam, 2018. https://bit.ly/3nqOnmd (letöltve: 2022.07.21.)

[79] SHANGPING Wang - YINGLONG Zhang - YALING Zhang.: A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems; Sisy2020, IEEE Access, 2018. https://bit.ly/3dXTebd (letöltve: 2022.07.21.)

[80] LÁSZLÓ Fazekas.: InterPlanetary File System (IPFS) avagy fájlrendszer a blokklánchoz; 2018. https://bit.ly/2XeSnuF (letöltve: 2022.07.21.)

[81] MUQADDAS Naz - FAHAD A. Al-zahrani - RABIYA Khalid - NADEEM Javaid - ALI Mustafa Qamar - MUHAMMAD Khalil Afzal.: A Secure Data Sharing Platform Using Blockchain and Interplanetary File System; Journal, Sustainability, 2019. https://bit.ly/2PvE3g9 (letöltve: 2022.07.21.)

[82] BÁLINT Krisztián.: Iskolai adatbázis biztonság; Kiberbiztonság – Cybersecurity 2. Óbudai Egyetem, Biztonságtudományi Doktori iskola, 247 p. pp. 95-105. 11 p. 2019. https://bit.ly/3AZvOye (letöltve: 2022.07.21.)

[83] NANCY Albinson - CHERIAN Thomas - MICHAEL Rohrig - YANG Chu.: Delottie, Protecting against the changing cybersecurity risk landscape; 2019. https://bit.ly/3k1gWEo (letöltve: 2022.07.21.)

[84] WALTERS Kluwer.: 2004. évi LXXIX. törvény az Európa Tanács Budapesten; Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről. 2004. https://bit.ly/3aH4kPZ (letöltve: 2022.07.21.)

[85] GYARAKI Réka.: Számítógépes bűncselekmények és az ellenük való védekezés; 175-189. 2014. https://bit.ly/3aNXQPd (letöltve: 2022.07.21.)

[86] ANDRÉ Vitalis.: Kamerás megfigyelés, biztonság és szabadságjogok; Információs Társadalom 2.1 56-57, 2002. https://bit.ly/3vtuLAF (letöltve: 2022.07.21.)

[87] ERDŐS Gabriella.: Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén; Corvinus Egyetem Budapest, ISSN: 2416-0415, 2020. https://bit.ly/3xwkaXq (letöltve: 2022.07.21.)

[88] POK László.: 7 fontos feladat a kihirdetett GDPR salátatörvény alapján; 2019. https://bit.ly/3PGRIKD (letöltve: 2022.07.21.)

[89] RÉTI Várszagi és Társai Ügyvédi Iroda.: GDPR Salad Leaf 1. - Rules for Camera Surveillance and Electronic Access Control Relaxed GDPR Salátalevél 1, Lazultak a kamerás megfigyelés és az elektronikus beléptetés szabályai; 2019. https://bit.ly/31x8F2s (letöltve: 2022.07.21.)

[90] MIHOLA Réka.: GDPR Salátalevél 1. – Lazultak a kamerás megfigyelés és az elektronikus beléptetés szabályai; 2019. https://bit.ly/3OjtF3j (letöltve: 2022.07.21.)

[91] SLUŽBENI Glasnik.: 97/08 törvény a videó megfigyelőrendszerek alkalmazásáról Szerbiában; 2022. https://bit.ly/3aWtyNB (letöltve: 2022.07.21.)

[92] PARAGRAF.: Személyes adatvédelmi törvény; 2022. https://bit.ly/3q8L4AZ (letöltve: 2022.07.21.)

[93] BÁLINT Krisztián.: The connection of a Blockchain with Students' Attendance Register based on Security Cameras; IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY 2021) 191 p. pp. 67-70, 4 p. 2021. https://bit.ly/3PjMe8l (letöltve: 2022.07.21.)

[94] ABINAYA G - PREKSHA Kothari - ALEX Pavithran KP - MANASI Biswas - FARHEEN Khan.: Block Chain Based Decentralized Cloud Storage; International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-4, April, 2019. https://bit.ly/2QDL8vB (letöltve: 2022.07.21.)

[95] TURÁNYI Noémi.: Okos szerződések, avagy okos életünk következő lépcsőfoka; 2018. https://bit.ly/3eKri7S (letöltve: 2022.07.21.)

[96] COINMIXED.: Smart Contract – Mik azok az okos szerződések; 2018. https://bit.ly/32wZzoL (letöltve: 2020.02.27.)

[97] CSITEI Béla.: Okos szerződések; Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányi Kar, Civilsztikai Tanszék, 2019. https://bit.ly/3nuCHie (letöltve: 2022.07.21.)

[98] PRINCE Waqas Khan – YUNG Cheol Byun - NAMJE Park.: A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities; Journal Electronics, 2020. https://bit.ly/2R6TVWC (letöltve: 2022.07.21.)

[99] KATHI Ferenc.: Szakdolgozat - Hash Függvények; Debreceni Egyetemi Informatikai Kar, 2009. https://bit.ly/3gM6OjG (letöltve: 2022.07.21.)

[100] CSAJBÓK Zoltán.: Azonosságon alapuló titkosítás korházi információs rendszerben; Informatika a felsőoktatásban, Debrecen, 227 p. p. 136. 2008. https://bit.ly/3ROb42n (letöltve: 2022.07.21.)

[101] DANIEL Kats.: A Gentle Introduction to Attribute-Based Encryption; 2019. https://bit.ly/2B3iU5O (letöltve: 2022.07.21.)

[102] EARL Bebbie.: A társadalomtudományi kutatás gyakorlata; VI. kiadás. Balassi Kiadó Budapest. 2001, https://bit.ly/3mD02hW (letöltve: 2022.07.21.)

[103] ÓBUDAI Egyetem.: Az Óbudai Egyetem Tanulmányi és Vizsgaszabályzata III Kötet; Budapest, 2021. https://bit.ly/3NJCl3y (letöltve: 2022.07.21.)

[104] ISAAC Asimov.: Citatum; Tudományos Idézetek. 1992. https://bit.ly/3PpHJtl (letöltve: 2022.07.21.)

A KUTATÁSOMMAL KAPCSOLATOS TUDOMÁNYOS MUNKÁIM

BÁLINT Krisztián.: Modern, Decentralized Blockchain-Based Solutions for Saving Video Footage; IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY 2020) Danvers (MA), Amerikai Egyesült Államok: IEEE, 185 p. pp. 11-14, 4 p. 2020. https://bit.ly/3eDB7X7 (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Connecting Bitcoin Blockchain with Digital Learning Chain Structure in Education; Acta Polytechnica Hungarica, Volume 16, Issue Number 1, 2019. https://bit.ly/3gND7yP (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Iskolai biztonság fontosága; Berek Hetven: Egy élet a hadtudomány és a művészet szolgálatában, a hetvenéves Berek Lajos professzor és szobrászművész köszöntése; Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, ISBN:9789634491576, pp. 33-42, 10 p. 2019. https://bit.ly/3RYtQEq (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Composition of an Automated Attendance Register of Students by Security Cameras, as Part of Smart City; Interdisciplinary Description of Complex Systems, Budapest, Óbudai University, Smart City, pp. 27-36, 10p. 2016. https://bit.ly/3nUPXgX (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Biztonsági kamerákon alapuló hallgatói jelenléti ívkészítő rendszer analitikai funkciói; Rendészet-Tudomány-Aktualitások, A rendészettudomány a fiatal kutatók szemével, Doktoranduszok Országos Szövetsége Rendészettudományi Osztály Budapest, pp. 42-49, 8 p. 2021. https://bit.ly/3ADXZCG (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Biztonsági kamerákon és blokklánc technológián alapuló hallgatói jelenléti ívkészítő rendszer működésének modellje és annak felépítése; XXIV. Tavaszi Szél Konferencia 2021, Budapest, Magyarország: Doktoranduszok Országos Szövetsége (DOSZ) 667 p. pp. 217-217, 1 p. 2021. https://bit.ly/3oeSeUD (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Modern, Blockchain-Based Fire Protection Solutions Through In-School Security Cameras; Hadmérnök, Volume Number: 15, Issue: 4, Pages: 5-14. 2020. https://bit.ly/3sW7u8Q (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Lehetséges modern információbiztonsági megoldások az iskolai biztonsági kamerarendszerek tároló architektúráját illetően; Kiberbiztonság - Cyber Security: Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból, Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, pp. 141-153., 12 p. 2018. https://bit.ly/3xv9U1D (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a Universities' Modern Security Cameras; Acta Polytechnica Hungarica, DOI: 10.12700/APH.18.2.2021.2.7, Volume 18, Issue Number 2, 2021. https://bit.ly/3IQgLZH (letöltve: 2022.07.21.)

BÁLINT Krisztián.: Iskolai adatbázis biztonság; Kiberbiztonság – Cybersecurity 2. Óbudai Egyetem, Biztonságtudományi Doktori iskola, 247 p. pp. 95-105. 11 p. 2019. https://bit.ly/3AZvOye (letöltve: 2022.07.21.)

BÁLINT Krisztián.: The connection of a Blockchain with Students' Attendance Register based on Security Cameras; IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY 2021) 191 p. pp. 67-70, 4 p. 2021. https://bit.ly/3PjMe8l (letöltve: 2022.07.21.)

RÖVIDÍTÉSJEGYZÉK

CCTV - Zártláncú videó megfigyelő rendszer, Closed-Circuit Television,

NVR – Hálózati videórögzítő, Netword Video Recorder

DVR – Digitális videófelvevő egység, Digital Video Recorder

ATM – Bankautomata, Automated Telles Machine,

ÓUDSC – Létrehozott egyetemi blokklánc neve, Óbudai Egyetem adattároló blokklánc, Óbudai University Data Storage Chain,

MP- Felbontóképesség, Megapixel,

HD – Nagyfelbontás, 720p, High Definition,

Full HD - Teljes nagyfelbontás, 1080p, Full High Definition

MJPEG – Mozgókép tömörítási eljárás, Motion Joint Photographic Experts Group,

H.264 - Mozgókép képtömörítási eljárás, MPEG-4 Part 10 vagy MPEG-4 AVC,

H.265, HEVC - Mozgókép képtömörítási eljárás, High Efficiency Video Coding,

NETD – Termikus érzékenység, Noise Equivalent Temperature Difference,

mK – Termodinamikai hőmérséklet mértékegysége, MiliKelvin,

IoT – Dolgok Internete, Internet of Things,

PoW- Konszenzus algoritmus típusa, Proof of Work,

PoS - Konszenzus algoritmus típusa, Proof of Stake,

EKG – Elektrokardiográfia, Electrocardiogram,

DAS – Közvetlenül csatolt tárolás, Direct Attached Storage,

NAS – Hálózatra csatolt tároló, Network Attached Storage

SAN – Tároló hálózat, Storage Area Network,

RAID - Tárolási technológia, Redundant Array of Independent Disk,

iSCSI – Internet SCSI tárolóhálózat, Internet Small Computer Systems Interface,

CDB – Parancsleíró blokk, Command Descriptor Block,

LUN – Logikai egységszám, Logical Unit Number

ABE - Attribútum alapú titkosítás, Attribute-Based Encryption,

PKG - Privát Kulcsú Generátor, Privat Key Generator,

IBE - Azonosító alapú titkosítás, Identity Based Encryption,

DDoS – Szolgáltatásmegtagadással járó támadás, Distributed Denial of Service Attack,

IPFS – Peer-to-Peer alapon működő tartalomcentrikus blokktároló, Interplanetary File System,

DHT – Elosztott Hash táblák, Distributed Hash Tables,

GDPR - Általános adatvédelmi rendelet, General Data Protection Regulation,

SHA – Kriptográfiai Hash függvény, Secure Hash Algorithm,

NIST - Egyesült Államok Nemzeti Szabvány és Technológia Hivatala, National Institute of Standards and Technology,

NSA – Nemzetbiztonsági Ügynökség, National Security Agency,

SHA-2 - Kriptográfiai Hash függvény 2, Secure Hash Algorithm 2,

SHA 512 - Kriptográfiai Hash függvény 512, Secure Hash Algorithm 512,

ABE - Attribútum alapú titkosítás, Attribute-Based Encryption,

IBE - Azonosító alapú titkosítás, Identity Based Encryption,

IP – Internet protokoll, Internet Protocol,

PKG - Privát Kulcsú Generátor, Privat Key Generator,

Mbps - Sávszélesség/adatátviteli sebesség mértékegysége, Megabit per secundum,

HDD - Merevlemez, Hard Disk.

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Köszönettel tartozom a szüleimnek, **Bálint Jánosnak** és **Máriának** a sok segítségükért, támogatásukért és biztatásukért.

Feleségemnek, **Dr. Bálint Mónikának**, aki nem egy esetben ellátott jó tanácsaival, valamint a türelméért a doktori tanulmányom alatt. Mindvégig támogatott és biztatott, amelyért hálás vagyok.

Prof. Dr. Berek Lajos tanár úrnak a mentorálásért és a folyamatos segítőkészségéért. A mentorom nagyban hozzájárult ahhoz, hogy a kutatásaim eredményesek legyenek.

Prof. Dr. Rajnai Zoltán dékán úrnak, aki a doktori képzésem mind a négy éve alatt segítőkész volt velem szemben és támogatott.

Habil Dr. Berek Tamás kutatói jó tanácsainak köszönhetően, amely nagyban hozzájárult ahhoz, hogy számos színvonalas konferencián publikálhassak.

Dr. Szabó Gyula egyetemi oktatónak, aki számos kutatói jó tanáccsal és ötlettel ellátott.

Dr. Kovács Tibor egyetemi docens és tanszékvezető szakmai támogatásáért.

Levay Katalin és **Dr. Hronyec Erika** ügyintézőknek, akik nélkül az egyetemi adminisztráció világában elvesztem volna.

Továbbá szeretném megköszönni a Biztonságtudományi Doktori Iskola és Óbudai Egyetem vezetésének, hogy támogatták a kutatásomat, valamint a szigorlati és nyilvános bizottság tagjainak az értékes építő jellegű kritikáikat.