Tudományos Diákköri Konferencia  
Egyéb tudományok: Informatikai szekció  
Budapest, 2020. november 27.  
Kodolányi János Egyetem

***Két eszköz közti adatátviteli lehetőségek áttekintése a biztonság szempontjából.***

***Jelige: Fő a biztonság!***

***2020. november 27.***

Tartalomjegyzék

[Bevezetés 3](#_Toc56203922)

[Kiindulási helyzet 3](#_Toc56203923)

[Motiváció 4](#_Toc56203924)

[Rövid feladat-ismertetés 4](#_Toc56203925)

[Célcsoport 4](#_Toc56203926)

[Hasznosság 6](#_Toc56203927)

[Adatok – a szakirodalmi háttér alapján 7](#_Toc56203928)

[Adatgyűjtés 7](#_Toc56203929)

[Adatok feldolgozása 10](#_Toc56203930)

[Sorszámozás 10](#_Toc56203931)

[Kombinatorikai tér 13](#_Toc56203932)

[Adatok feldolgozása mesterséges intelligenciával 14](#_Toc56203933)

[Validitás vizsgálat 15](#_Toc56203934)

[Adatok rövid elemzése 16](#_Toc56203935)

[Naiv becslési táblázat 17](#_Toc56203936)

[Eredmények 18](#_Toc56203937)

[Nyertes objektumok – modell becslési táblázat 18](#_Toc56203938)

[Nyertes objektumok – naiv becslési táblázat 20](#_Toc56203939)

[Riport1 21](#_Toc56203940)

[Riport2 21](#_Toc56203941)

[Riport3 22](#_Toc56203942)

[Összefoglalás 23](#_Toc56203943)

[Rezümé – HU 23](#_Toc56203944)

[Rezümé – EN 24](#_Toc56203945)

[Források 25](#_Toc56203946)

[Melléklet 26](#_Toc56203947)

[Rövidítések jegyzéke 26](#_Toc56203948)

[Ábrák jegyzéke 27](#_Toc56203949)

# Bevezetés

A bevezetésben ismertetésre kerül a kutatás motivációja, rövid bemutatása, felvezetése és célcsoportja.

## Kiindulási helyzet

1. ábra - [Teamviewer](https://play.google.com/store/apps/details?id=com.teamviewer.teamviewer.market.mobile&hl=en_US&gl=US), távoli elérés és irányítás

Az informatikában leginkább a rendszergazdai munkakörben vagy egyéb szerverekkel dolgozó cégeknél fontos, hogy a lehető legegyszerűbben és leggyorsabban tudják kezelni a szervereket és az egyéb számítógépeket. Erre van egy, az informatikában bármilyen területen, akár otthoni felhasználásban is gyakran használt módszer, ez a távoli elérés. Ennek segítségével interneten keresztül, a közelség, helyhez kötöttség igénye nélkül és a kábelek közötti elveszettség elkerülésével lehet kezelni szervereket, adatokat mozgatni eszközök között és akár a teljes irányítást átvenni a számítógépek fölött. Ez gyakran hasznos tud lenni például, ha bármilyen szoftveres probléma adódik a számítógéppel. A jelenlegi COVID-helyzetben kifejezetten előnyös, ha nem kell a számítógéppel elbuszozni a szervízig, de az autóból se kell fogyasztani a benzint és egy informatikában jártas ismerőst se kell személyesen áthívni, hogy segítsen. Mindössze engedélyezni kell, hogy távolról hozzáférjenek az eszközünkhöz és ők otthonról, a saját gépükön keresztül, a saját komfortzónájukból való kilépés nélkül tudnak majd nekünk segíteni. Az 1. ábra egy ilyen alkalmazást, a Teamviewer-t ábrázolja. Ezek a megoldások mindenki számára sokkal kényelmesebbek, de egyben veszélyesebbek is, mint az internet/hálózat nélküli megoldások. így, ha valaki ezt a kényelmes megoldást választja, figyelnie kell a biztonságra is. Ezen a téren nehezebb dolga van egy hétköznapi felhasználónak, de néha még a szakértők is csak azért használnak adott programokat, mert valamikor azt mondták nekik, hogy az a jó és azóta hozzászoktak a használatához, de valójában semmit nem tudnak arról, hogy tényleg biztonságos programot használnak-e, esetleg, hogy nem lenne-e valami jobb, biztonságosabb megoldás.

## Motiváció

Az én esetemben egy egyetemi projekt volt hasonló, használtam a megszokott alkalmazásokat és protokollokat, de valójában nem tudtam miért használom azt, amit és hogy van-e biztonságosabb megoldás. Az alap ötlet is ebből származik, **vajon mi a legbiztonságosabb távoli elérési-irányítási program vagy protokoll?**

A konkrét szakmaiság mellett elméleti kérdésként az is felmerült, hogy a legbiztonságosabb objektum problémájának megoldása mennyire általánosítható, mennyire automatizálható, mennyire context free, vagyis az általam kidolgozott megoldás szolgálhat-e a jövőben keretrendszerként hasonló problémák kezeléséhez?

A dolgozat tudományos vonatkozása tehát többrétegű:

* A Knuth-i elv mentén (mely szerint tudás az, ami forráskódba átírható) megoldást találni a legjobb objektum kiválasztásának kihívására,
* S mindenezt minél inkább context free
* és automatizálható módon…

## Rövid feladat-ismertetés

Egy induktív szakértői rendszer (az online hasonlóságelemzés: <https://miau.my-x.hu/myx-free/coco/index.html> ) segítségével végzünk összehasonlítást tizenkét (2+10) darab távoli elérési módszer között 2\*128 szcenárió keretében, és állapítjuk meg a győzteseket. Azért esett a választásom a hasonlóságelemzésre, mert arra a kérdésre, hogy lehet-e számos objektum másként egyforma, más módszerekkel csak szubjektív válaszok adhatók, s ezen szubjektivitás kizárja a knuth-i elvet, a context free és automatizálási célokat.

## Célcsoport

Ahogy az „Kiindulási helyzet” fejezetben már kifejtésre került, rengeteg helyen, valójában lassan a munkák legnagyobb részében hasznos lehet a két eszköz közötti kapcsolat, mint olyan, hiszen már majdnem mindenhol, ha nem mindenhol, használnak számítógépeket és/vagy egyéb informatikai eszközöket így a távoli elérés rengeteg ember munkáját könnyítheti meg és teheti kényelmesebbé. A jelenlegi vírushelyzetben pedig kiemelten fontos szerepet játszhat, ha az emberek távolról is képesek dolgozni olyan programokkal és adatokkal, melyek a saját eszközükön, otthon nem érhetőek el. Az adatok biztonsága pedig mind a cégek, mind az egyének felelőssége. Akár munkaügyben használ valaki ilyen megoldást. Magán területen is kifejezetten előnyös, ha a lehető legbiztonságosabb módszert használja az ember és így nem kerülnek az adatai illetéktelen kezekbe, esetleg veszik át az ember eszközei felett ismeretlenek az irányítást.

Mindezekből következik, hogy ezen ötlet megvalósítása rengeteg embernek lenne segítség, hogy biztonságban tudhassa adatait miközben kényelmesen, távolról dolgozik.

## Hasznosság

A startup-ok kapcsán immár közismert vélekedés, hogy ami mindenkinek jó, az senkinek sem igazán jó! Inkább legyen tehát egy szűkebb/kisebb célcsoport, ahol becsülhető egy adott szolgáltatás (jelen esetben robot-szakértői vélemény) ellenértéke, mint sem bizonytalan célcsoport-koncepcióval ne tudjunk célirányos marketinget folytatni.

Ezért a dolgozat elsődleges célcsoportja a nagy kattintás szám generálására és így bevételtermelésre esélyt adó közösségi média-fogyasztók azon köre, akik szeretik az összehasonlító elemzésekről szóló animációkat. A második célcsoport a szaklapok, akik számára a most még rel. lassan kiérlelődő szakvélemény a jövőben számos egyéb objektumkörben tud majd hatékonyan szakvéleményt termelni a szerzőknek járó honorárium fejében.

# Adatok – a szakirodalmi háttér alapján

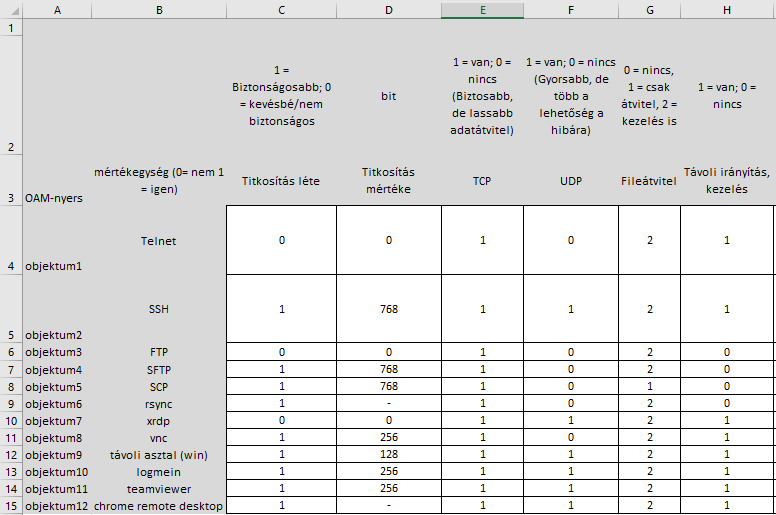
Ebben a részben bemutatásra kerül minden összegyűjtött adat és a kezelésük, feldolgozásuk menete.

## Adatgyűjtés

A korábban említett tizenkét (2+10) lehetőség a saját és szakmai környezetem véleményére alapozva a leginkább ismertnek és használtnak tűnt szoftverek kerültek kiválasztásra és elemzésre. (későbbiekben objektumok) Szintén saját és szakmai környezetem véleményére alapozva tizenöt biztonsággal kapcsolatban álló jelenség lett kiemelve és ezekkel kapcsolatban lettek adatok gyűjtve objektumonként. (későbbiekben attribútumok) Az objektumokkal való egymáshoz képesti túlzottan sok/kevés foglalkozás/adatkeresgélés elkerülése miatt minden objektumnál csak a hivatalos weboldalt, az adott objektumhoz tartozó magyar és angol nyelvű Wikipédia cikkeket, valamint saját, már meglévő tudásomat használtam fel. (Ezek linkjei a dokumentum végén a források/referenciák fejezetben megtalálhatóak). A rel. kevés forrásoldal elemzése helyenként adathiányt eredményezett melyekkel így a többitől eltérő módszerrel kellett foglalkozni.

A kiválasztott objektumok közé tartozik a két leggyakrabban használt és iskolákban is tanított parancssoros[[1]](#footnote-1) felületű (CLI)[[2]](#footnote-2) lehetőség, ez a Telnet és az SSH[[3]](#footnote-3). Ezeken kívül van tíz olyan objektumunk is, amelyeknél nem csak parancssoros elérésre van lehetőség. Ezek pedig az FTP[[4]](#footnote-4) SFTP[[5]](#footnote-5) SCP[[6]](#footnote-6), rsync, xrdp, vnc, távoli asztal (win), logmein, teamviewer, chrome remote desktop.

A hozzájuk tartozó attribútumok pedig a következőek (2. és 3. ábra): használ-e titkosítást az adott objektum, amennyiben igen, milyen mértékűt. (C és D oszlopok – 2. ábra) Itt a telnet az FTP és az xrdp kapott egy 0-ást, tekintve, hogy ők nem használnak titkosítást. Az rsync-nél és a chrome remote desktopnál nem volt adat a megadott helyeken a titkosítás mértékéről, csak annyit tudunk, hogy használ titkosítást. A legnagyobb érték 768 bit volt, ezt az SSH az SFTP és az SCP kapták. Ezt követte a 256 bites titkosítás mely a vnc-re a logmein-re és a teamviewerre volt igaz. A leggyengébb a 128 bites titkosítás volt, melyet csak a távoli asztal (win) (későbbiekben csak távoli asztal) kapott. Itt egyértelműen az kap jobb értékelést, amelyiknek erősebb a titkosítása. (legerősebb innen: 768bit) Milyen TCP/IP[[7]](#footnote-7) protokollcsomagbéli[[8]](#footnote-8)[[9]](#footnote-9) protokollt használ, pontosabban két részre lett bontva, hogy van-e lehetőség a TCP[[10]](#footnote-10) használatára és hogy van-e lehetőség UDP[[11]](#footnote-11) használatára. (E és F oszlopok – 2. ábra) Itt a TCP használata a biztonságosabb adatvesztés szempontból, hiszen a TCP ellenőrzi az adatok épségét. A TCP-t az összes még az UDP-t csak az SSH az xrdp a távoli asztal a logmein a teamviewer és a chrome remote desktop támogatják. Megvizsgálásra került az is, hogy van-e lehetőség file átvitelre és ha van akkor csak a fileok mozgatása lehetséges a két eszköz között, vagy azoknak kezelésére[[12]](#footnote-12) is van lehetőség. (G oszlop – 2. ábra) Itt az SCP volt az egyetlen, aki csak fájlmozgatásra volt képes, az összes többi a kezelésükre is. Ehhez hasonlóan megvizsgálásra került az is, hogy csak adatok kezelésére vagy az eszköz kezelésére, irányítására is van-e lehetőség. (H oszlop – 2. ábra) Ennél az attribútumnál az FTP az SFTP az SCP és az xrdp kaptak 0-ást, mert ők csak fileműveletekre képesek, az eszköz bárminemű irányítására nem. A biztonsághoz kapcsolódhat a keletkezés éve is mely felveti a kérdést, hogy az újabb, azaz frissebb tudással és technológiával elkészített objektumok a biztonságosabbak, vagy pedig a régebbi, sok hibát és így hibajavítást megélt lehetőségek. (I oszlop – 3. ábra) Én nem tudnék egyértelmű választ adni erre a kérdésre magamtól, ahogy szerintem sokan mások sem, így mindkét lehetőséget meg kell vizsgálni. Itt a legrégebbi objektum a Telnet, hiszen ennek a megjelenési időpontja 1969. Ezt követi az FTP 1971-gyel, majd sorrendben az SCP (1983), az SSH (1995), az rsync (1996), az SFTP holtversenyben a távoli asztallal (1998), a vnc (1999), a logmein (2003), az xrdp (2004), a teamviewer (2005) majd végül a chrome remote desktop (2011). Ezt követte a sebesség értékelése. Itt általánosítottam, azaz a leglassabb lett a legbiztonságosabb. (J oszlop – 3. ábra) Ez az esetek legnagyobb százalékában igaz is, egy-két kivételtől eltekintve. Három sebességre lett bontva, ezek értékei pedig a következők: 3 – gyors, 2 – közepes, 1 – lassú. Ezek alapján az FTP 3-ast kapott, az SFTP 1-est (itt is látszik, a titkosítás mentes FTP gyors még a 768 bites titkosítással rendelkező SFTP lassú), az SCP 2-est, az rsync 3-ast. Az xrdp, a vnc, a távoli asztal, a logmein, a teamviewer és a chrome remote desktop pedig mind 2-es értékelést kaptak. Multiplatformosság terén mindegyik 1-est (azaz van rá lehetőség) kapott, az xrdp-n kívül. (K oszlop – 3. ábra) Kétirányú kommunikációra az összes vizsgált objektum képes, és az összes full-duplex így mind 2-es értékelést kaptak. (L oszlop – 3. ábra) Az ablakkezelő technika a Telnet és az SSH kivételével mindnél jelen van. (M oszlop – 3. ábra) Késleltetésnél szintén a Telnet és az SSH képeznek kivételt, náluk ez alacsony még mindenhol máshol magas. (N oszlop – 3. ábra) Hibaellenőrzés minden vizsgált objektumnál megtörténik. (O oszlop – 3. ábra) Proxy támogatás csak az xrdp és a távoli asztal objektumoknál nincs. (P oszlop – 3. ábra) Mobil applikációt pedig az SCP xrdp és a távoli asztal kivételével mindegyikhez találunk. (Q oszlop – 3. ábra).



2. ábra - Forrás: Saját táblázat – objektum-attribútum mátrix első fele (nyers adatok)

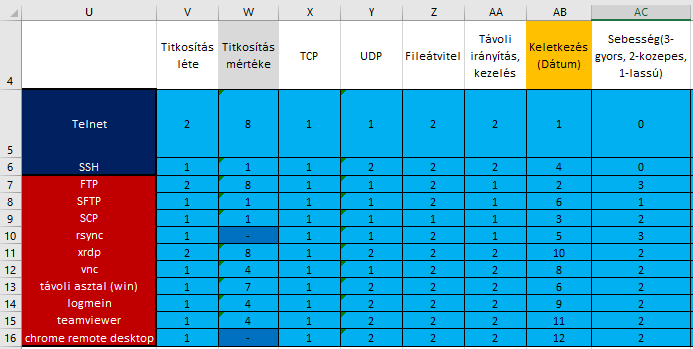
## Adatok feldolgozása

3. ábra - Forrás: saját táblázat - objektum-attribútum mátrix második fele (nyers adatok) – A sorfejléc azonos a 2. ábráéval

Ebben a fejezetben a már összegyűjtött adatok feldolgozásának menete lesz látható.

### Sorszámozás

Az összegyűjtött nyers adatok alapján rangsorolásra (vö. 4. és 5. ábra) került az összes objektum attribútumonként és a későbbiekben ezekkel a sorszámokkal folytatódott a munka.

A legtöbb helyen egy szimpla „HA” Excel függvény lett használva, mivel a legtöbb attribútum alatt csak kettő vagy három különböző érték szerepel, így ez volt talán a legjobb megoldás. Amely attribútumoknál sokkal több érték szerepelt, ott a „SORSZÁM” Excel függvény került alkalmazásra. Ilyenek voltak a „Titkosítás mértéke” és a „Keletkezés (Dátum)” attribútumok. A „Titkosítás léte” részben azok kaptak 1-es sorszámot, amelyekben volt titkosítás, azaz a korábbi táblázatban is 1-es értéket kaptak, még kettes értéket a korábbi táblázat 0-ásai kapták, azaz amelyik objektumok nem használnak titkosítást. Ide tartozott a Telnet az FTP és az xrdp. (V oszlop – 4. ábra) A titkosítás mértékénél négy különböző értékkel találkoztunk, de mivel itt „SORSZÁM” függvény volt használva, így a sorszámok nem első, második, harmadik és negyedik értékek lettek, hanem első, negyedik hetedik és nyolcadik – a holtversenyek sorszám-eltoló hatásai miatt. Nyolcadik helyen végzett az a néhány objektum, akinél nem volt titkosítás. Hetedik helyen csak a távoli asztal végzett a maga 128 bites titkosításával. Negyedik helyezettek lettek a 256 bites titkosítással rendelkező objektumok, ezek pedig a vnc, a logmein és a teamviewer. Első helyezést az SSH az SFTP és az SCP kaptak a 768 bites titkosításuk miatt. Az rsync és a chrome remote desktop adathiánya pedig megköveteli, hogy megvizsgáljuk az eredményeket minden elérhető helyezéssel, azaz mindkét helyen 4 lehetőségünk lesz. (W oszlop – 4. ábra) Mivel a TCP-t az összes támogatja, így mindegyik objektum első helyezést kapott ebben a vizsgálatban, ez az attribútum így egyáltalán nem befolyásolja a végeredményt. (X oszlop – 4. ábra) AZ UDP-nél az adathelyességet tudjuk vizsgálni, mint biztonsági tényező, mivel az UDP nem ellenőrzi az adatok épségét. Emiatt az UDP-t támogató objektumok itt második helyen végeztek, míg akik nem támogatják azok az első helyet kapták meg. AZ UDP-t támogató objektumok pedig a Telnet, az FTP, az SFTP, az SCP, az rsync és a vnc voltak. (Y oszlop – 4. ábra) File átvitelnél, akik kezelni is tudják a fileokat és nem csak mozgatni őket, azok nagyobb biztonsági kockázatot jelentenek, azaz ők kerültek a második helyre. Az első helyen csak az SCP végzett, mivel ő az egyetlen, aki nem képes a fileok kezelésére, csak mozgatására. (Z oszlop – 4. ábra) Távoli irányításnál/kezelésnél az jelent kevesebb biztonsági kockázatot, aki erre nem képes, szóval ezek az objektumok kapták az első helyezést. Ezek az FTP, SFTP, SCP és az rsync voltak. (AA oszlop – 4. ábra) A keletkezés dátuma a korábban leírtak alapján két módon is elemezhető, az egyik megtalálható a „4. ábra” AB oszlopában. A másik vizsgálati irány ennek tükrözött változata, azaz a 3. ábrán az első helyen lévő objektum lesz a tizenkettedik helyen és a tizenkettedik pedig az első helyen, köztük mindegyik sorszám megfordul ehhez a kettőhöz hasonlóan. Az AC oszlopban (4. ábra), a sebességeknél az első helyet a leglassabb objektum kapta és a 3. helyet a leggyorsabb, a korábban említett hozzáállás miatt. A Telnet és az SSH 0-ás értéket kapott itt, mivel náluk nem számít különösebben semmit a sebesség, lévén parancssorosok, parancsvégrehajtásra valóak. Multiplatformosságnál az okoz többlet kockázatot, ahol erre lehetőség van, így az xrdp (11. sor) kapta az egyetlen első helyezést és minden más objektum csak második lett. (AD oszlop – 5. ábra) A két irányú kommunikáció szintén nem befolyásolja az eredményt lévén mindegyik full-duplex. (AE oszlop – 5. ábra) Az ablakkezelő technikánál biztonsági kockázatként azt lehet felhozni, hogy amennyiben erre nincs lehetőség, azaz csak parancssoros elérés van, mint a Telnet és az SSH esetében, akkor sokkal könnyebb bármit elhibázni vagy bármi olyanba belenyúlni, ami adatvesztéssel jár, így ez kapja a második helyezést, még az ablakkezelő technikával rendelkező objektumoké az első hely. (AF oszlop – 5. ábra) Késleltetés terén az első helyen azok az objektumok végeztek melyeknél a késleltetés kisebb, így az adatok időben érkeznek meg. (AG oszlop – 5. ábra) Az AH oszlop (5. ábra) nem befojásolja az eredményt, mivel az összes vizsgált objektumnál van hibaellenőrzés, mind első helyen végeznének. Az AI oszlopban (5. ábra) azok az objektumok szerepelnek az első helyen, melyek támogatják a Proxyt. Amelyek nem támogatják, azok a második helyen szerepelnek, ezek az xrdp és a távoli asztal. Az AJ oszlopban (5. ábra) nagyobb biztonsági kockázatot jelent, ha van lehetőség mobilról is használni az objektumokat, így azok kaptak első helyezést, melyeknél erre nincs lehetőség. Ezek pedig az SCP az xrdp és a távoli asztal.

4. ábra - Forrás: Saját táblázat - objektum-attribútum mátrix első fele (sorszámozott adatok)

5. ábra - Forrás: Saját táblázat - objektum-attribútum mátrix második fele (sorszámozott adatok)

### Kombinatorikai tér

Mint az a 3. ábrán már látható volt, van néhány speciális esetünk, ilyen például az adathiány kezelése, és a keletkezési dátum-iránya. Ezek miatt több különböző esetet is meg kell vizsgálnunk annak érdekében, hogy az adathiány eredményekre gyakorolt esetleges hatását fel lehessen ismerni (vö. érzékenység-vizsgálat).

A keletkezési dátum kettő eshetőséget ad nekünk, van a direkt irány-variáns, melynél az újabb objektumot vesszük biztonságosabbnak és van az inverz irány-variáns, ahol a régebbi objektumot tekintjük biztonságosabbnak. Emberi/szakértői szemmel nézve mindkét irány-definícióban van helyesség és logikailag mindkettő igaznak tűnhet – de ideális esetben csak ezek egyikét illik preferálni. Az már egy más kérdés, mit is mondhat erre egy mesterséges intelligencia, de erről még szó fog esni később az Eredmények fejezetben.

Ezen kívül korábban volt már szó két hiányos adatról, melyek négy-négy lehetséges helyettesítési értékkel bírnak. Mivel minden lehetséges kombinációt meg kell vizsgálnunk így jelenleg 4\*4\*2 = 32 lehetőségnél tartunk. Az informatikában kicsit is jártas ember első ránézésre látja, hogy van egy kis különbség néhány vizsgált objektum között, a legnagyobb eltérések mentén két csoportra tudjuk bontani az objektumokat. A mi esetünkben ez a két csoport a „Mind” és a „Csak” nevet kapták. A „Mind” csoportban szerepel mind a 12 objektum, míg a „Csak” csoportban csak 10 objektum található. Itt kivettük a vizsgálatokból a Telnetet és az SSH-t. Ez szintén két új lehetőséget ad, azaz jelenleg 32\*2 = 64-nél tartunk.

Ezen kívül szükséges még megvizsgálni az eredmények validitását, melyben egy mesterséges intelligencia és az Excel együttesen segédkeztek. Ez szintén ad két újabb lehetőséget, így a jelenlegi állás 64\*2 = 128. Ebből a 128 lehetőségből jön ki egy modell becslés táblázat, ezen kívül elkészítésre került egy ugyanekkora méretű (szóval már 128\*2 = 256) naiv értékelési táblázat is összehasonlítási céllal, ahol a naiv értékelés nem valami rosszat jelent, csak annyit, hogy nem optimalizált, szemben a robot modell-számításaival.

### Adatok feldolgozása mesterséges intelligenciával

7. ábra - Forrás: Saját táblázat - modell-becslési táblázat inverz dátum-irány variánssal

6. ábra - Forrás: Saját táblázat - modell-becslési táblázat direkt dátum-irány variánssal

A 4. és 5. ábra adatai egy mesterséges intelligencia[[13]](#footnote-13) (későbbiekben MI) segítségével kerültek feldolgozásra. Az első tizenhat (16) változat eredményeit összesítve (validitás elemzés után) az 6. ábrán lehet megtekinteni. Itt csak az direkt irány-variáns van vizsgálva a tizenhat különböző adathiányvariáns mellett. A 7. ábrán szintén a tizenhat különböző adathiányvariáns vizsgálata történt meg, csak itt inverz irány-variánssal. A 6. és 7. ábrán a C oszlop a dátum-irány variánsokat tartalmazza. A kék szín a direkt (6. ábra) a narancssárga (7. ábra) pedig az inverz dátum-irány variánsok adatai előtt áll. Az első sorban látható a két csoport elválasztása is a kék szöveg jelöli a „Mind” csoportot, a piros háttér pedig a „Csak” csoportot. A D3-as cellától az O34-es celláig tartó intervallumon találjuk az MI által feldolgozott és a validitás vizsgálaton átesett értékeket. A fehér háttérrel rendelkező cellák invalidak. Minden más szín soronként az értékek nagyságától függően látható. (sötét zöld – Legmagasabb érték, vörös – legalacsonyabb érték).

### Validitás vizsgálat

9. ábra - Forrás: Saját táblázat - modell-becslési táblázat a tükörértékekkel (ellenőrő tábla)

8. ábra - Forrás: Saját táblázat - modell-becslési táblázat validitás ellenőrzés nélkül

A validitás ellenőrzéshez ugyanaz az MI lett használva, csak a korábbi adatok (eredeti adatok validitás ellenőrzés nélkül a 8. ábrán láthatóak) ellentétével lettek lefuttatva a számítások. (9. ábra) A tükörmátrixok elkészítésénél csak az alap sorszámok lettek megfordítva, egy „SORSZÁM” excel függvény használatával. Ezt követően ezek az adatok is mekerültek a korábban használt MI-ba és a már ismert módon elkészült az ellenőrző táblázat. (9. ábra).

A validitás megállapításához elsősorban az MI által adott adatok közül egy ide ki nem emelt érték került felhasználásra. AZ MI-ban az adatok lefuttatása után egy eléggé nagy adattömeget kaptunk vissza, ahol megtalálható volt egy „delta” oszlopfejléccel rendelkező adat. Az eredeti és a tükör számításból származó delta értékek összeszorzása után amennyiben az eredmény nullánál kisebb lett, azaz negatív eredményt dobott, az eredmény validnak számított, amennyiben az eredmény pozitív lett, csak akkor került megvizsgálásrra a 8. és 9. ábra viszonya. Ha az közös helyen szereplő értékek 1000 körül voltak (999-nél nagyobb és 1001-nél kisebb) akkor kerekítési hibának lett tekintve az invaliditása és a végső táblázatba valid-ként került be. A validitás vizsgálat eredményei számadatok nélkül a 10. ábrán tekinthetőek meg.

### Adatok rövid elemzése

10. ábra - Forrás: Saját táblázat - validitási táblázat számadatok nélkül

Ha megvizsgáljuk a validitási táblázatot (10. ábra), ránézésre az szűrhető le, hogy a direkt és az inverz részeken közel ugyanannyi invalid érték található, ráadásul ezeknek a legnagyobb része az SSH objektumhoz tartozik. A dátum-idő irányvariáns változásával várható volt sok változás, a táblázatokat vizsgálva azt láthatjuk, hogy a sorrend változása különösen nagy hatással volt a legtöbb objektumra és sokakat majdnem teljesen vagy teljesen az ellentétére változtatott. Ezt a 6. és a 7. ábrát szemrevételezve vehetjük észre. A direk irány zöld és sárga értékei elvörösödtek, a vörösek pedig a zöld irányába mozdultak el, persze itt is látni egy-két olyan objektumot, ami kivételt képez, azaz alig észrevehetően változott csak, például az SFTP és az SCP.

### Naiv becslési táblázat

11. ábra – Forrás: saját táblázat - Naiv becslési táblázat

A naiv becslési adatmátrixról korábban esett már szó. Ez az adathalmaz ellenőrzési céllal lett létrehozva. Az adatait a korábbi sorszám mátrixból kapta. (4. és 5. ábra) Szintén minden dátum-irány variáns és minden adathiány variáns megvizsgálásra került. Az egyéni eredményeket az adott részek eredményeinek átlagából lettek kiszámítva. (ÁTLAG) Excel függvény. Ezeknek a számításoknak az eredményeit összesítve a 11. ábrán lehet megtekinteni. Ebben a táblázatban, a modell becslésekkel ellentétben a kisebb értékek számítanak jobbnak.

# Eredmények

Ebben a részben előkerülnek a korábbi táblázatok által sikeresen előállított győztes objektumok és megfogalmazásra kerül néhány, az eredményekből levont következtetés.

## Nyertes objektumok – modell becslési táblázat

12. ábra - Forrás: Saját táblázat - összesített táblázat nyertes objektumokkal foglalkozó része - modell

A modell becslési táblázatoknál az egyéni eredmények kiszámítása mellett a győztes objektumokat is ki kell keresni és ki kell emelni. Ezt könnyedén meg lehet tenni, mivel minden adat és számítás az Excelben lett elvégezve, így továbbra is tudunk ebben, Excel függvényekkel dolgozni. Elsőként a legmagasabb értéket kell kiválasztani a már összegzett táblázatból. (6. és 7. ábra) Ezt egy egyszerű MAX függvénnyel tudjuk megtenni. Figyelni kell azonban arra, hogy két különböző csoporttal dolgozunk, így le kell futtatni ezt az összes elemen (Mind) és a Csak részen is. (P oszlop – Mind csoport legmagasabb értéke, Q oszlop – Csak csoport legmagasabb értéke – 12. ábra) (Például: P3 cella - ***=MAX(D3:O3)*** és Q3 cella - ***=MAX(F3:O3)*** – Ezek értelmezéséhez szükséges a visszatekintés a 6. és 7. ábrákra) Ezt követően ellenőrizni kell, hogy van-e holtverseny az első helyen. Ennek az eredményeit az S (Mind csoporthoz tartozó) és az U (Csak csoporthoz tartozó) oszlopokban lehet megtalálni. Ezt egy DARABTELI Excel függvénnyel lehet megtenni. (Például: S3 cella - ***=DARABTELI(D3:O3;P3),*** U3 cella - ***=DARABTELI(F3:O3;Q3)*** – Az értelmezéshez szükséges a visszatekintés a 6. és 7. ábrákra) Ennél a vizsgálatnál egy szerencsés forgatókönyv következett be, ugyanis nincs egy holtverseny sem. Mivel nincs több azonos értékű győztes így a győztes objektumok kigyűjtése megoldható egy egyszerű INDEX + HOL.VAN függvénypárral. (Például: R3 - ***=INDEX(D1:O1;HOL.VAN(P3;D3:O3;0))***, T3- ***=INDEX(F1:O1;HOL.VAN(Q3;F3:O3;0))*** – Az értelmezéséhez szükséges a visszatekintés a 6. és 7. ábrákra) Azt már szabad szemmel is látjuk, hogy elég egységes a győztes objektumok kiléte, minden esetben az SCP éri el a legmagasabb értékelést.

## Nyertes objektumok – naiv becslési táblázat

13. ábra - Saját táblázat - összesített táblázat nyertes objektumokkal foglalkozó része - naiv

A naiv becslési táblázat létrehozásáról már volt korábban szó. Az itteni eredmények (13. ábra) szintén a korábban említett módszerek alapján lettek elkészítve, annyi különbséggel, hogy a fentebb említett MAX függvény helyett itt MIN függvény került alkalmazásra. (Például: CT3 - ***=MIN(CH3:CS3)***, CU3 - ***=MIN(CJ3:CS3)***) Ezt a táblázat részletet a 11. ábra segítségével lehet tökéletesen értelmezni. Egészen tisztán látszik szabad szemmel is, hogy az itteni nyertes objektumok már közel sem mutatnak olyan stabil eredményt, mint a modell becsléses párjuk. Itt a direkt dátum-irány részben megjelenik több más győztes objektum is.

## Riport1

14. ábra - Forrás: Saját táblázat - Riport1 - invaliditási arányok dátum-irányonként

Az első riportban (14. ábra) az invaliditási arányok kerülnek elő dátum-irány variánsokként. A C oszlopban a direkt becslés adatai láthatóak. A C42-es cellába került a direkt dátum-irány variánsok invalid értékeinek százalékban mért értéke. A C41-es cellába a százalékos értékek mögött álló invalid értékek darabszáma található szintén a direkt dátum-irány variánsra vonatkozóan. Ugyanezen értékek az inverz dátum-irány variánsra a D42-es és D41-es cellában találhatóak. Az egyes riportról leolvasható, hogy a dátum-irány variánsok változása nem hat ki a validitásra.

## Riport2

15. ábra - Forrás: Saját táblázat - Riport2 - Győzelmek aránya dátum-irányonként és Csak-Mind csoportonként

A második riportban (15. ábra) a C és a D oszlopokban az inverz dátum-irány variánsokra vonatkozóan látható a Mind (C oszlop) és a Csak (D oszlop) részekre vonatkozó győzelmek aránya. A direkt dátum-irány variánsra a Mind rész győzelmi arányát az E, még a Csak rész győzelmi arányát az F oszlopban lehet látni. A négy darab 100%-os győzelmi arány után, melyből mind a négy az SCP-hez köthető, azt a következtetést vonhatjuk le, hogy se az adathiány, se a Csak-Mind csoportvariánsok, se a két dátum-irány variáns nincs hatással a győztes objektum kilétére. Ezek alapján azt gondolhatjuk, ha bármilyen új objektumot és/vagy attribútumot helyeznénk be, bármely oldal eredményeit nézhetnénk és választhatnánk, hiszen minden esetben helyes győztes objektumot kapunk.

## Riport3

16. ábra - Forrás: Saját táblázat - Riport3 - Naiv és Modell győztesek egyezésének aránya

A 16. ábrán, azaz a 3. riportban a modell becslések és a naiv becslések győztesei lettek összevetve és ezeknek az egyezéseinek az arányát lehet látni az 53. sorban Azt vehetjük észre, hogy az inverz dátum-irány variánsban 100%-os egyezés van a naiv és a modell becslések között a Mind és a Csak részben is. Ezzel szemben a direkt dátum-irány variánsban a Mind és a Csak részben is 0%-os egyezést látni. Ez az eredmény felborítja akorábban levont kövezkeztetést, miszerint mindegyik érték helyes lehet. Az itteni eredmények alapján az inverz dátum-irány variáns a biztosabb választás. Ez jelen helyzetben nem kifejezetten számít, azonban amint bekerül több objektum és attribútum, esetleg csak a naív értékelés lenne meg a későbbiobjektumokkal és attribútumokkal, akkor lényeges szerepet tölthet be a döntésben az, hogy tudjuk az inverz dátum-irány a biztosabb választás.

# Összefoglalás

## Rezümé – HU

A dolgozatban két eszköz (pl.: 2 asztali és/vagy szerver-számítógép) közti adatátviteli lehetőségek néhány (2+10 db) gyakran használt módszere kerül megvizsgálásra objektumként és kerül összehasonlításra egy induktív szakértői keretrendszer segítségével az objektumokról rendelkezésre álló attribútumok (15 db - egy attribútum esetén 2 adathelyen hiányos – 4-4 opciót kínáló) adatai alapján az attribútumok irány-variánsaira és a mesterséges intelligencia-alapú indukció minőségmenedzsmentjére is példát mutatva. A vizsgált szcenáriók száma, vagyis a kombinatorikai tér alapmérete 128 (2\* inverz variáns \* 2 irányvariáns \* 2 objektumhalmaz-variáns \* 16 adathiányvariáns) – mely úgy modellezett, mint naiv megoldásokat is jelent párhuzamosan (2\*128=256). Az OAM mérete: 12\*15. A szakértői keretrendszer képes az alapvető biztonsággal kapcsolatban álló jelenségek értékei alapján, több kombinatorikai megközelítésből megvizsgálni az objektumokat, majd modellválaszként adni az adott vizsgálati irány és preferenciák alapján talált győztest, azaz a legjobb objektumot. A 2+10 objektum (vö. Mind, illetve Csak rétegek) a Telnet, az SSH, illetve FTP, STFT, SCP, rsync, xrdp, vnc, távoli asztal (win), logmein, teamviewer és a chrome remote desktop. Biztonsággal kapcsolatos jelenségek (attribútumok) pedig a titkosítás megléte és ennek mértéke, az átvitelhez használt protokoll (TCP, UDP), fileátvitel lehetősége, távoli irányítás megléte, keletkezés ideje (dátum), melynél figyelembe lett véve két nézőpont is (újabb a jobb, régebbi a jobb), az átvitel sebessége, multiplatformosság, két irányú kommunikáció lehetősége, ablakkezelő technika megléte, késleltetés mértéke, hibaellenőrzés és proxy támogatás megléte és mobilapplikációs elérhetőség. A 128 modellezett szcenárió alapján a hasonlóságelemzés-párokra alapozó (context free) indukció keretében az alábbi rendszerszintű eredményekre derült fény: a dátum-irány variáns nem befolyásolja az invaliditási arányokat (riport1 – az objektum-invaliditás arányai dátum-irányonként). Könnyedén leszűrhető az is, hogy semmilyen variálás, se a dátum-irány variánsok változása, se az adathiány variánsok változása nem befolyásolja a végeredményt, a nyertes objektum 100%-ban az SCP lesz mindenhol. (riport2) Az anti-diszkriminatív elveket követő optimalizáló, induktív keretrendszer mellett készült egy naiv (nem optimalizáló), vagyis csak az attribútumok irányított sorszámértékeit átlagoló megoldáshalmaz is, mely mérete azonos a modellezett megoldáshalmazzal. Ha összevetjük a naiv becslések győzteseit a modell becslések győzteseivel, azt látjuk, hogy a direkt dátum-irány variánsoknál az egyezés a Mind és a csak részben is 0%-os, még ugyanez az érték az inverzeknél 100% Ebből azt a következtetést vonhatjuk le, hogy hiába egyező a győztes objektum mindenhol, az inverz irány ad biztosabb eredményt, ez a következtetés akkor lehetne fontos, ha bekerülne még néhány objektum és/vagy attribútum, vagy ha a naiv, átlagoló becslés eredményeit akarnánk alapul venni és nem a modellbecsléséit. (riport3)

## Rezümé – EN

The focus of the study is a comparison between a set (2+10) of well-known methods (as objects) to transferring files between two devices (e.g.: two desktop and/or server PC). An inductive expert system got involved into the combinatorial process to make comparisons between a rel. robust set of modelled and naïve scenarios, where the number of the defined attributes about the security of the transferring is 15. The number of modelled scenarios is 128 (4\*4\* data missing-variants, 2\* date-preference-variants, 2\* object conglomerations, 2\* validity). The size of an OAM is 12\*15. The inductive expert frame system is able to derive the potential winner(s) as the best (most secure) object(s). The 2+10 objects are (in two groups like All and Only) Telnet, SSH + FTP, STFT, SCP, rsync, xrdp, vnc, remote desktop connection (win), logmein, teamviewer and the chrome remote desktop. The 15 attributes about security are the type/availability of encryption and the strongness of this, used protocol (TCP, UDP), possibility for file transfer, remote control, release date where two preference-variants (the older the more secure, the newer the more secure) are available, speed of transmission, multiplatformity, two-way communication, window treatment technology, delay-characteristics, error checking, proxy support and the type/availability of a mobile application. The results of the analyses: the date-preference-variants do not affect the validity rates. (c.f. Riport1 object invalidity rates by date-preference-variants) We can see that too, the most secure object always be the same, nothing (date-preference-variants, validity, data missing-variants, object conglemerations) attect it. SCP has a 100% winning rate. (c.f. Riport2) We can notice that, the naive values make a 0% match with the model values in direct date-preference-variant and the same matches are 100% when we see the inverse date-preference-variant. This means the inverse date-preference-variant gives us a safer result. (c.f. Riport3)

# Források

<https://en.wikipedia.org/wiki/Telnet> - 2020.11.13

<https://hu.wikipedia.org/wiki/Telnet> - 2020.11.13

<https://www.ssh.com/ssh/telnet> - 2020.11.13

<https://en.wikipedia.org/wiki/SSH_(Secure_Shell)> – 2020.11.13

<https://www.ssh.com/> - 2020.11.13

<https://hu.wikipedia.org/wiki/Secure_Shell> - 2020.11.13

<https://en.wikipedia.org/wiki/File_Transfer_Protocol> - 2020.11.13

<https://hu.wikipedia.org/wiki/File_Transfer_Protocol> - 2020.11.13

<https://en.wikipedia.org/wiki/SFTP> - 2020.11.13

<https://en.wikipedia.org/wiki/Secure_file_transfer_program> - 2020.11.13

<https://en.wikipedia.org/wiki/Secure_copy_protocol> - 2020.11.13

<https://en.wikipedia.org/wiki/Rsync> - 2020.11.13

<http://xrdp.org/> - 2020.11.13

<https://en.wikipedia.org/wiki/Xrdp> - 2020.11.13

<https://en.wikipedia.org/wiki/Virtual_Network_Computing> - 2020.11.13

<https://www.realvnc.com/en/> - 2020.11.13

<https://en.wikipedia.org/wiki/Remote_Desktop_Protocol> - 2020.11.13

<https://www.logmein.com/home2#/> - 2020.11.13

<https://hu.wikipedia.org/wiki/LogMeIn> - 2020.11.13

<https://en.wikipedia.org/wiki/LogMeIn> - 2020.11.13

<https://www.teamviewer.com/en/> - 2020.11.13

<https://en.wikipedia.org/wiki/TeamViewer> - 2020.11.13

<https://remotedesktop.google.com/?pli=1> – 2020.11.13

<https://en.wikipedia.org/wiki/Chrome_Remote_Desktop> - 2020.11.13

<https://rsync.samba.org/> - 2020.11.13

# Melléklet

## Rövidítések jegyzéke

* CLI – Console Line Interface – Parancssoros felület
* SSH -Secure Shell
* FTP – File Transfer Protocol – File átviteli protokoll
* SFTP – Secure File Transfer Protocol – Biztonságos file átviteli protokoll
* SCP – Secure Copy Protocol
* TCP/IP - Transmission Control Protocol / Internet Protocol
* TCP - Transmission Control Protocol
* UDP - User Datagram Protocol
* rel. - Relatív
* vö. – Vesd össze
* MI – Mesterséges Intelligencia
* VNC – Virtual Network Computing

## Ábrák jegyzéke

[1. ábra - Teamviewer, távoli elérés és irányítás 3](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205380)

[2. ábra - Forrás: Saját táblázat – objektum-attribútum mátrix első fele (nyers adatok) 9](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205381)

[3. ábra - Forrás: saját táblázat - objektum-attribútum mátrix második fele (nyers adatok) – A sorfejléc azonos a 2. ábráéval 10](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205382)

[4. ábra - Forrás: Saját táblázat - objektum-attribútum mátrix első fele (sorszámozott adatok) 12](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205383)

[5. ábra - Forrás: Saját táblázat - objektum-attribútum mátrix második fele (sorszámozott adatok) 12](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205384)

[6. ábra - Forrás: Saját táblázat - modell-becslési táblázat direkt dátum-irány variánssal 14](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205385)

[7. ábra - Forrás: Saját táblázat - modell-becslési táblázat inverz dátum-irány variánssal 14](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205386)

[9. ábra - Forrás: Saját táblázat - modell-becslési táblázat a tükörértékekkel (ellenőrő tábla) 15](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205387)

[8. ábra - Forrás: Saját táblázat - modell-becslési táblázat validitás ellenőrzés nélkül 15](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205388)

[10. ábra - Forrás: Saját táblázat - validitási táblázat számadatok nélkül 16](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205389)

[11. ábra – Forrás: saját táblázat - Naiv becslési táblázat 17](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205390)

[12. ábra - Forrás: Saját táblázat - összesített táblázat nyertes objektumokkal foglalkozó része - modell 18](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205391)

[13. ábra - Saját táblázat - összesített táblázat nyertes objektumokkal foglalkozó része - naiv 20](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205392)

[14. ábra - Forrás: Saját táblázat - Riport1 - invaliditási arányok dátum-irányonként 21](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205393)

[15. ábra - Forrás: Saját táblázat - Riport2 - Győzelmek aránya dátum-irányonként és Csak-Mind csoportonként 21](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205394)

[16. ábra - Forrás: Saját táblázat - Riport3 - Naiv és Modell győztesek egyezésének aránya 22](file:///D:\School\KJE\TDK\TDK_Fő_a_biztonság%20(1).docx#_Toc56205395)

1. Parancssor - szöveges/konzolos felület melyben kódokkal/parancsokkal lehet navigálni és parancsokat kiadni az eszköznek [↑](#footnote-ref-1)
2. Console Line Interface - parancssoros felület [↑](#footnote-ref-2)
3. Secure Shell [↑](#footnote-ref-3)
4. File Trasfer Protocol [↑](#footnote-ref-4)
5. Secure File Transfer Protocol [↑](#footnote-ref-5)
6. Secure Copy Protocol [↑](#footnote-ref-6)
7. Transmission Control Protocol / Internet Protocol [↑](#footnote-ref-7)
8. TCP/IP protokollcsomag – „Az internet működését biztosító protokollcsomag megnevezése.” \* [link](https://pcforum.hu/szotar/TCP%2FIP) [↑](#footnote-ref-8)
9. Protokollcsomag – „Egymással összefüggésben lévő protokollok halmaza” \* [link](https://pcforum.hu/szotar/protokollcsomag) [↑](#footnote-ref-9)
10. Transmission Control Protocol – ellenőrzi az adatok épségét [↑](#footnote-ref-10)
11. User Datagram Protocol – nem ellenőrzi az adatok épségét [↑](#footnote-ref-11)
12. szerkesztés, törlés, futtatás… [↑](#footnote-ref-12)
13. A használt MI linkje: <https://miau.my-x.hu/myx-free/coco/index.html> - COCO Y0 [↑](#footnote-ref-13)