

---

# **Zsarolóvírus-támadások időkritikus felismerése gépi tanulás alkalmazási lehetőségeinek vizsgálatával centralizált fájl tárolási környezetekben**

---

Doktori (PhD) értekezés tézisei

**Arányi Gábor**

Témavezető: Dr. Szücs Veronika

Pannon Egyetem  
Műszaki Informatikai Kar  
Informatikai Tudományok Doktori Iskola

**2026**

## Motiváció és célkitűzések

A digitalizáció térnyerésével párhuzamosan a különböző szervezetek, intézmények és vállalatok működése egyre inkább az informatikai rendszerekre támaszkodik. Ezzel a digitális adatvagyon, illetve az ezekhez kapcsolódó szoftverkörnyezetek sok szervezet számára a legfontosabb technológiai értéké válnak. Az informatikai rendszerek komplexitásának növekedése, a felhasználói oldalon tapasztalható biztonságtudatossági hiányosságok, a szakmai kompetenciák hiánya, valamint az elavult vagy nem megfelelően karbantartott rendszerek egyaránt hozzájárulnak a kibertámadásoknak való kitettséghez. A zsarolóvírustámadások napjaink talán legsúlyosabb kiberbiztonsági fenyegetését jelentik, amit a támadási módszerek folyamatos fejlődése és a Ransomware-as-a-Service (RaaS) platformok elterjedése még inkább fokoz. A korábban magas szintű szakértelmet igénylő támadások végrehajtása mára lényegesen egyszerűbbé vált, miközben az egészségügyi és oktatási intézmények, valamint a mikro-, kis- és középvállalkozások elavult informatikai infrastruktúrájuk, korlátozott erőforrásaik és a rendelkezésre álló szakértelem hiánya miatt egyre kiszolgáltatottabb célpontokká váltak. Az olyan védelmi megoldások, mint például a Next Generation (NG) tűzfalak, a behatolásjelző és megelőző rendszerek (IDS/IPS), a biztonsági információ- és eseménykezelő (SIEM) platformok, az adatszivárgás megelőző (DLP) szoftverek és az antivírus megoldások ugyan fontos szerepet töltenek be az informatikai infrastruktúrák védelmében, azonban önmagukban sokszor nem elegendők a zsarolóvírustámadások hatékony kivédéséhez és a károk minimalizálásához. A hangsúly gyakran a háttárvédelmen és a kliens eszközök védelmén van, miközben a centralizáltan tárolt adatvagyon védelme háttérbe szorul, holott kritikus terület lenne a tárolt adatokon végzett műveletek felügyelete, illetve az adatok gyors helyreállításának megoldása. A kritikus adatok védelme érdekében olyan költséghatékony és könnyen integrálható megoldásokra van szükség, amelyek a végpontvédelmi rendszerektől függetlenül képesek biztosítani a zsarolóvírustámadások gyors felismerését, az adatok biztonságos tárolását és visszaállítását.

A kutatás egyik célja egy olyan többretegű, platformfüggetlen védelmi modell koncepcionális kidolgozása (Anti-Ransomware Defense System), amely a végpontvédelmektől független, könnyen integrálható és komplex védelmi képességekkel rendelkezik. A másik kutatási cél az ARDS modell részét képező fájlkiszolgáló oldali védelmi megoldás gyakorlati alkalmazhatóságának igazolása referenciaalapú teljesítményvizsgálattal, valamint a fájlműveleti szekvenciákra alapuló, felügyelt gépi tanulást alkalmazó, alacsony erőforrásigényű, közel valós idejű zsarolóvírus-detektálási módszer vizsgálatával.

## Új tudományos eredmények

A következő lista négy tézisben foglalja össze az új tudományos eredményeimet.

### 1. Tézis

Igazolható, hogy a heterogén kliens–szerver architektúrák fájlátviteli teljesítménye páronként definiált, dinamikus referencia-alapú relatív teljesítménymutató alkalmazásával objektív módon összevethető, ahol az összehasonlíthatóságot az azonos művelet sor mellett mért átviteli sebességek egymáshoz viszonyított aránya biztosítja, nem pedig abszolút teljesítményértékek.

### 1. Tézis alátámasztása

A heterogén kliens–szerver architektúrák vizsgálata során megállapítható volt, hogy az abszolút fájlátviteli teljesítményértékek még azonos hardverkörnyezet és fájl tartalmak mellett is jelentős eltéréseket mutathatnak a szoftverkörnyezetek függvényében. Ez a jelenség megnehezíti az eltérő konfigurációk objektív összehasonlítását, mivel az abszolút mérési eredmények nem különíthetők el egyértelműen a környezeti sajátosságoktól. A heterogén környezetekben végzett teljesítménymérések összehasonlíthatósági problémájának kezelésére a kutatás során egy új, általam kidolgozott, páronként definiált, dinamikus referencia-alapú relatív teljesítménymutatót vezettem be, amely platformfüggetlen módon alkalmazható, reprodukálható mérési eljárást biztosít, és megfelelő referencia-rendszer definiálása mellett általánosítható. A mutató a mérések során az azonos fájlátviteli irányok (olvasás, írás) mellett mért átviteli sebességek egymáshoz viszonyított arányán alapult, így nem az abszolút átviteli sebességeket tekinti elsődleges összehasonlítási alapnak, hanem minden vizsgált konfiguráció teljesítményét egy előre definiált referencia-rendszerhez viszonyítja. Ez mérsékli a platformfüggő sajátosságok összehasonlítást torzító hatását, és lehetővé teszi különböző operációs rendszerek, fájlrendszerek és adatvédelmi mechanizmusok által nyújtott fájlátviteli teljesítmény egységes skálán történő értékelését. Fontos kiemelni továbbá, hogy a kidolgozott módszerrel az egyes konfigurációk közötti teljesítményváltozások – például rendszerhangolás vagy védelmi funkciók bevezetése – következetesen nyomon követhetővé válnak.

A kutatás tudományos hozzájárulása nem kizárólag egy FreeBSD-alapú konfiguráció teljesítményének meghatározásában rejlik, hanem egy olyan általánosítható referencia-

alapú értékelési módszer kidolgozásában, amely heterogén szolgáltatáskörnyezetek objektív összehasonlítását teszi lehetővé. A módszer alkalmazásával különböző operációs rendszerek, fájlrendszerek, titkosítási eljárások és adattárolási architektúrák teljesítménye egy-egy mérőszám segítségével értékelhető. A megközelítés ezért nemcsak a jelen kutatásban vizsgált konfigurációkra alkalmazható, hanem általános módszertani keretet biztosít jövőbeli rendszer-összehasonlító vizsgálatok számára is.

A vizsgálatok során meghatározott relatív teljesítménymutató valamennyi vizsgált konfiguráció esetében konzisztensen értelmezhető eredményeket szolgáltatott, és lehetővé tette az eltérő operációs rendszerek, fájlrendszerek és adatvédelmi konfigurációk objektív összehasonlítását. A különböző mérési sorozatokban kapott eredmények igazolták, hogy a referencia-alapú mutató alkalmas a teljesítményváltozások számszerű követésére, ezáltal alátámasztja a tézisben megfogalmazott módszertani állítást.

### **Az 1. tézist alátámasztó saját publikációk:**

[S1] Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS-Anti-Ransomware Defense System Model-Based on the Systematic Review of Worldwide Ransomware Attacks. *Applied Sciences-Basel*, 11(13). <http://doi.org/10.3390/app11136070>, SJR Q2, WoS Q2 IF: 2,838

[S2] Arányi, G.; Vathy-Fogarassy, Á.; Szücs, V.; Evaluation of a New-Concept Secure File Server Solution. *Future Internet 2024*, MDPI, 16, 306. <https://doi.org/10.3390/fi16090306>, SJR Q2, WoS Q2 IF: 3,6

### **2. Tézis**

Igazolható, hogy centralizált fájlkiszolgáló környezet esetén, virtualizált kliens–szerver infrastruktúrában a szerveroldali időbélyeggel ellátott, idősorfolytonos fájlműveleti naplóadatok megfelelő előszűréssel, normalizálással és egy másodperces időablakra történő aggregációval olyan strukturált idősoros reprezentációvá alakíthatók, amely alapján bizonyos gépi tanulási modellek alkalmasak kliensoldali információ nélkül is a teljes titkosítást alkalmazó zsarolóvírusok által generált intenzív fájlműveleti aktivitás kvázi valós idejű hatékony detektálására.

### **2. Tézis alátámasztása és korlátai**

A vizsgálat olyan klasszikus, teljes titkosítást alkalmazó zsarolóvírusokra (Ryuk, WannaCry, NotPetya, LockBit, TeslaCrypt) terjedt ki, amelyek működésük során intenzív létre-

hozási, átnevezési és törlési fájlműveleteket generálnak. A mérések centralizált fájlkiszolgálást megvalósító, virtualizált kliens–szerver infrastruktúrában történtek. Az elemzés idősorfolytonos, egy másodperces időablakokra aggregált adatsoron zajlott, ahol a referenciaállapotot tipikus irodai felhasználói fájlhasználati minták alapján definiáltam. A mérések igazolták, hogy a fájlkiszolgáló oldalon keletkező, időbélyeggel ellátott fájlműveleti naplóadatok önmagukban elegendő információt hordoznak a vizsgált zsarolóvírus-tevékenységekhez kapcsolódó intenzitás- és mintázatváltozások kimutatásához. Normál működés során a létrehozási, átnevezési és törlési műveletek száma és időbeli eloszlása stabil referenciaállapotot alkotott, míg zsarolóvírus-tevékenység esetén rövid idő alatt nagyságrendi intenzitásváltozás és jellegzetes mintázateltérés jelent meg. Az előszűrés és az időablakos aggregáció eredményeként a naplóadatok nem nyers eseményhalmazként, hanem struktúrált, idősorfolytonos numerikus reprezentációként álltak rendelkezésre. Ez az adatrepresentáció közvetlenül felhasználható bemenetet biztosított a felügyelt gépi tanulási modellek számára, megalapozva a zsarolóvírus-tevékenység automatikus detektálását. Az egymást követő időablakokban aggregált eseménysorok alapján a fájlműveleti aktivitás időbeli lefutása folyamatosan nyomon követhetővé vált, így az észlelési folyamat nem utólagos elemzésként, hanem kvázi valós idejű megfigyelésként volt értelmezhető.

A kutatás módszertani hozzájárulása egy olyan szerveroldali, időablakos adatrepresentáció kidolgozása, amely kizárólag fájlkiszolgálói naplóadatokra támaszkodva biztosítja a zsarolóvírus-tevékenység gépi tanulással történő detektálásához szükséges bemeneti reprezentációt. A módszer nem kötődik konkrét gépi tanulási algoritmushoz, ezért különböző osztályozási modellek bemeneteként is alkalmazható.

A következtetések olyan centralizált fájlkiszolgáló környezetekre érvényesek, ahol a fájlműveletek időbélyeggel naplózhatók, és a támadók intenzív fájlrendszer-szintű titkosítási folyamatot hajtanak végre. A vizsgálat nem terjedt ki olyan zsarolóvírus-változatokra, amelyek minimális fájlműveleti aktivitással dolgoznak, vagy nem alkalmaznak titkosítást. A referenciaállapot tipikus irodai munkaterhelés mellett került kialakításra, ezért a hosszú távú üzemeltetés során jelentkező felhasználói viselkedésváltozás, valamint az újabb ransomware-családokra (concept drift) történő általánosíthatóság vizsgálata további kutatási irányt jelent. Emellett a jelen kutatás időkerete nem tette lehetővé a módszer hosszabb időtartamra vonatkozó validálását, ezért annak stabilitása és adaptivitása hosszabb üzemeltetési periódusokban további empirikus vizsgálatot igényel.

### 3. Tézis

Igazolható, hogy a normál felhasználói aktivitás és a teljes titkosítást alkalmazó zsarolóvírusok által kiváltott intenzív fájlműveleti mintázatok a vizsgált környezetben bináris osztályozási problémaként kezelhetők és klasszikus, valamint ensemble gépi tanulási módszerekkel a támadás időkritikus lefutásához illeszkedő döntési késleltetés mellett hatékonyan detektálhatók.

### 3. Tézis alátámasztása

A kutatás során a fájlkiszolgáló oldalon keletkező, időbélyeggel ellátott fájlműveleti naplóadatokra vonatkozóan olyan előfeldolgozási eljárást dolgoztam ki, amely előszűrést és egy másodperces időablakok szerinti aggregációt alkalmazott. Az adatelőkészítés eredményeként a létrehozási, átnevezési és törlési fájlműveletek nem nyers eseménysorként, hanem strukturált, idősorfolytonos numerikus reprezentációként álltak rendelkezésre, amely közvetlenül felhasználható bemenetet biztosított a felügyelt gépi tanulási modellek számára.

A referenciaállapotot különböző munkakörökhöz tartozó, tipikus irodai fájlhasználati minták alapján definiáltam. Normál működés során a fájlműveletek intenzitása és időbeli eloszlása stabil tartományban maradt, míg a vizsgált zsarolóvírusok (Ryuk, WannaCry, NotPetya, LockBit, TeslaCrypt) működése során rövid idő alatt nagyságrendi intenzitásnövekedés, valamint jól elkülöníthető időbeli mintázatváltozás jelentkezett. Ezek az eltérések nem elszigetelt eseményekként, hanem egymást követő időablakokon keresztül fennálló viselkedési mintázatként jelentek meg, amely lehetővé tette a normál és a támadással érintett időszakok egyértelmű elkülönítését. Mivel a kutatás célja a zsarolóvírus-tevékenység jelenlétének felismerése volt, nem pedig az egyes kártevőcsaládok azonosítása, a detektálási feladat bináris osztályozási problémaként volt kezelhető.

A strukturált adatrepresentáción végzett vizsgálatok igazolták, hogy mind a klasszikus, mind az ensemble gépi tanulási modellek alkalmasak a normál és a támadással érintett időablakok elkülönítésére. A hiperparaméter-optimalizálást követően valamennyi vizsgált modell 0,84 feletti érzékenységet ért el, míg az XGBoost modell 0,919-es értékkel kiemelkedett a többi modell közül. Ez a tesztadatkészlet 209 támadással érintett másodpercére vetítve 192 esetben helyes eredményt jelent. Az XGBoost emellett a legkedvezőbb kompromisszumot nyújtotta az érzékenység, a precision, és a hamis pozitív arány között, valamint a költségalapú értékelésnél is a legjobbnak bizonyult.

A mérések azt is igazolták, hogy a döntési folyamat időigénye nagyságrendileg megfelelő a zsarolóvírus-támadások időkritikus észleléséhez. Az osztályozás végrehajtásához

szükséges idő a legjobb teljesítményt nyújtó XGBoost modell esetében 392 időablakhoz tartozó bemeneti adatsor feldolgozásánál 0,93 ms volt, míg a többi modellnél 0,19 ms és 3,41 ms közötti értékeket mértem. Az időablakos feldolgozás és a modellek alacsony számítási igénye lehetővé tette, hogy az osztályozás eredménye az adatgyűjtést követően gyakorlatilag azonnal rendelkezésre álljon, miközben az erőforrásigény nem haladta meg a kis- és középvállalati környezetekben alkalmazott általános célú szerverek kapacitását.

A vizsgálatok alapján így igazolható, hogy a normál felhasználói aktivitás és a fájlrendszer-szintű ransomware-ek által kiváltott intenzív fájlműveleti mintázatok a vizsgált környezetben bináris osztályozási feladatként kezelhetők, és megfelelő adatelőkészítés esetén klasszikus, illetve ensemble gépi tanulási módszerekkel a támadások időkritikus lefutásához illeszkedő döntési késleltetés mellett hatékonyan detektálhatók.

A következtetések a vizsgálatban szereplő teljes titkosítást alkalmazó zsarolóvírusokra, valamint centralizált, virtualizált fájlkiszolgáló infrastruktúrára érvényesek. A referenciaállapot egy tipikus irodai munkaterhelés mellett került kialakításra. A kutatás nem terjedt ki a hosszú távú üzemeltetés során fellépő felhasználói viselkedésváltozás kezelésére, illetve a módszer több hónapos vagy éves időtávú validálására. Nem került vizsgálatra továbbá a később megjelenő, jelentősen eltérő működési karakterisztikájú ransomware-változatokra történő általánosíthatóság sem (concept drift vizsgálata), ezért ezek a kérdések további kutatási irányt jelentenek.

## **A 2. és 3. téziseket alátámasztó saját publikációk:**

[S1] Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS-Anti-Ransomware Defense System Model-Based on the Systematic Review of Worldwide Ransomware Attacks. Applied Sciences-Basel, 11(13). <http://doi.org/10.3390/app11136070> SJR Q2, WoS Q2 IF: 2,838

[S3] Arányi, G; Miseta, T; Szücs V., Ransomware Detection Based on Server-side File Operation Logs using Machine Learning. Journal on Information Security, Advances in Information Forensics and Security; Springer, 2025. <https://doi.org/10.1186/s13635-026-00229-7> SJR Q2, WoS Q2 IF: 2,1

## **4. Tézis**

Igazolható, hogy a vizsgált klasszikus, valamint ensemble gépi tanulási modellek gyakorlati használhatóságának megítéléséhez önmagában egyetlen teljesítménymutató nem elegendő, és a pontosság, az F1-pontszám, az érzékenység, a specificitás, a keveredési

mátrix, valamint a költség-alapú értékelés együttes alkalmazása átfogó és gyakorlati szempontokat szem előtt tartó összehasonlíthatóságot biztosít.

#### **4. Tézis alátámasztása**

A kutatás során végzett vizsgálatok rámutattak arra, hogy a zsarolóvírus-tevékenység detektálása esetén a gyakorlati használhatóság megítélése nem alapozható egyetlen teljesítménymutatóra. Különösen kiegyensúlyozatlan osztályeloszlás mellett a pontosság önmagában félrevezető képet adhat a modell teljesítményéről, mivel nem tükrözi a különböző típusú osztályozási hibák eltérő súlyú következményeit. A keveredési mátrix elemzése lehetővé tette a hamis pozitív és hamis negatív döntések arányának feltárását, míg az érzékenység és a specificitás vizsgálata rávilágított a detektálási képesség és a téves riasztások közötti kompromisszumokra. Az F1-pontszám ezek együttes figyelembevételével szolgált összegzett mutatóként, azonban önmagában ez sem bizonyult elegendőnek a gyakorlati alkalmazhatóság megítéléséhez. A költség alapú értékelés alkalmazása lehetővé tette, hogy a téves osztályozási eredményeket súlyozva tudjuk összehasonlítani a modellek teljesítményét. Így szemléltethető volt, hogy az egyes osztályozási hibák milyen mértékű károkozást jelentenének egy valós környezetben. Az eredmények alapján megállapítható, hogy a pontosság, az F1-pontszám, az érzékenység, a specificitás, a keveredési mátrix és a költség alapú értékelés együttes alkalmazása egy alkalmas megközelítés ahhoz, hogy a különböző gépi tanulási modellek teljesítményét összehasonlíthassuk és a gyakorlati használat szempontjából értelmezhető módon megítélhessük. A kutatás tudományos újdonsága annak igazolása, hogy a zsarolóvírusok detektálásához használt modellek értékelése többkritériumos döntési problémaként kezelhető, amelyben a modellek gyakorlati alkalmassága a klasszikus teljesítménymutatók és a költség-alapú értékelés integrált alkalmazásával megalapozottan megítélhető.

#### **A 4. tézist alátámasztó saját publikáció:**

[S3] Arányi, G; Miseta, T; Szücs V., Ransomware Detection Based on Server-side File Operation Logs using Machine Learning. Journal on Information Security, Advances in Information Forensics and Security; Springer, 2025. <https://doi.org/10.1186/s13635-026-00229-7> SJR Q2, WoS Q2 IF: 2,1

## Az új tudományos eredmények felhasználása

A kutatás eredményei hozzájárulhatnak a korlátozott erőforrásokkal rendelkező mikro-, kis- és középvállalkozások, valamint más centralizált adattárolást alkalmazó szervezetek zsarolóvírusok elleni védelmének fejlesztéséhez. A kidolgozott referenciaalapú teljesítményértékelési módszer általános módszertani eszközként alkalmazható heterogén informatikai környezetek összehasonlító vizsgálatára, míg a szerveroldali fájlműveleti naplókra alapuló, gépi tanulást alkalmazó detektálási megközelítés a meglévő mentési és helyreállítási megoldásokat kiegészítve képes lehet támogatni a zsarolóvírus-támadások korai felismerését és lehetővé teheti az incidensekre adott gyors válaszokat. További kutatások tárgyát képezheti például a fejlett titkosítási stratégiákat alkalmazó víruscsaládokon keresztül történő validálás, a valós üzemi környezetben való kiértékelés, a mélytanulási modellek alkalmazhatóságának vizsgálata, valamint a detektálási események felhasználása az automatizált mentési és helyreállítási folyamatok támogatására. További kutatási lehetőséget jelent az olvasási műveletek elemzésének bevonása, amely elősegítheti az adatszivárgással járó támadások korábbi felismerését is.

## További publikációk

Magyar Tudományos Művek Tára (MTMT) személyes kutatói oldal:

<https://m2.mtmt.hu/api/author/10069952>

Szücs, Veronika ; Arányi, Gábor ; Dávid, Ákos; Security Awareness of HCI in DigitAll Reality, Acta Polytechnica Hungarica 22 : 6 pp. 9-23. , 15 p. (2025).DOI:

10.12700/APH.22.6.2025.6.2 , SJR Q2, WoS Q2 IF: 1,8

Szücs, V., Arányi, G., & Dávid, Á. (2021). Security awareness of HCI in DigitAll Reality. In 12th IEEE International Conference on Cognitive Infocommunications (pp. 1095–1096)

Veronika, Szücs, Gábor, Arányi, Ágnes, Vathy-Fogarassy (2022). Security of IT systems in healthcare institutions. Az egészségügyi informatika COVID előtt és COVID után - A XXXV. Neumann Kollokvium konferencia kiadványa (pp. 45–50)

Arányi, G., Szücs, V. (2023). IoT related security issues and black-box testing experiences in a smart lighting system. International Scientific Journal Security & Future, VII(2), pp. 61–64.

Arányi, G., Kocsis, T., Marsi, T., & Szarvák, A. (2020). Kibertéri Fenyegetések. Budapest: Nemzeti Közszerződési Egyetem, Közigazgatási Továbbképzési Intézet