

Opponensi vélemény

Arányi Gábor

„Zsarolóvírus-támadások időkritikus felismerése gépi tanulás alkalmazási lehetőségeinek vizsgálatával centralizált fájl tárolási környezetekben”

című doktori (PhD) értekezéséről

Az értekezés témája, aktualitása és általános értékelése

A zsarolóvírus-támadások napjaink egyik legsúlyosabb, jelentős gazdasági és működési károkat okozó kiberbiztonsági fenyegetését jelentik. A támadások fejlődése, a zsarolóvírus-szolgáltatási modellek elterjedése, valamint a kritikus infrastruktúrákat, egészségügyi és oktatási intézményeket, illetve kis- és középvállalkozásokat érintő incidensek indokoltá teszik olyan védelmi megközelítések kutatását, amelyek nem kizárólag az ismert kártevők felismerésére, hanem a támadások viselkedési jellemzőinek detektálására, a gyors incidensválaszra és az adatvagyon helyreállíthatóságának biztosítására is alkalmasak.

Arányi Gábor értekezése ebbe a kutatási irányba illeszkedik. A dolgozat különösen értékes jellemzője a gyakorlati és mérnöki szemlélet, valamint az empirikus vizsgálatokra helyezett hangsúly. A szerző nem pusztán elméleti modellt mutat be, hanem konkrét infrastruktúrát alakít ki, teljesítményméréseket végez, saját naplózási és adatfeldolgozási környezetet hoz létre, továbbá több klasszikus és ensemble gépi tanulási modell összehasonlító értékelését végzi el.

A dolgozat kutatási íve több egymásra épülő területet fog össze. A szerző először a hazai kis- és középvállalkozások informatikai biztonsági helyzetét vizsgálja kérdőíves interjúk segítségével, majd bemutatja az ARDS védelmi koncepciót és annak fájl kiszolgálói megvalósítását, végül pedig szerveroldali fájl műveleti naplók alapján vizsgálja a zsarolóvírus-tevékenység gépi tanúlással történő időkritikus felismerésének lehetőségét.

Az értekezés korábbi változatához kapcsolódó opponensi észrevételek egyik fontos eleme volt, hogy e három kutatási terület tudományos kapcsolata és az egyes eredmények önálló újdonságértéke nem minden esetben vált kellően világossá. A végleges értekezés ezen a téren jelentős előrelépést mutat. A szerző egyértelműbben elkülöníti a mérnöki implementációt a módszertani és tudományos eredményektől, pontosabban határozza meg állításainak érvényességi tartományát, részletesebben tárgyalja kutatásának korlátait, és lényegesen precízebben fogalmazza meg a doktori téziseket. A dolgozat végén önállóan foglalkozik az eredmények tudományos pozicionálásával és a nemzetközi szakirodalom eredményeivel történő összevetésével is.

Mindezek következtében az értekezés jelenlegi változata véleményem szerint koherens, tudományosan értékelhető és doktori értekezésként megfelelő színvonalú munkának tekinthető.

A kutatás módszertani és tartalmi értékelése

A dolgozat egyik erőssége a módszertani tudatosság. A szakirodalom feldolgozásában a szerző a PRISMA módszertani keretet alkalmazza, külön figyelmet fordít a reprodukálhatóságra, a

teljesítménymérések során fellépő bizonytalanságokra, valamint a különböző mérési környezetek összehasonlíthatóságának problémájára.

A kis- és középvállalkozások körében végzett kérdőíves kutatás megfelelően megalapozza a vizsgált gyakorlati problémát, ugyanakkor a szerző helyesen korlátozza az abból levonható következtetések általánosíthatóságát. Az adatfelvétel a COVID-19 járvány időszakában történt, amely a távoli munkavégzés, a felhőszolgáltatások és a távoli hozzáférési megoldások gyors elterjedése miatt sajátos informatikai környezetet teremtett. A végleges értekezés már részletesen reflektál erre a korlátra, és arra is, hogy azóta az MFA, az EDR/MDR szolgáltatások, az immutable backup megoldások és az európai kiberbiztonsági szabályozás fejlődése jelentősen módosította a KKV-k működési környezetét. E reflexív megközelítést kifejezetten pozitívnak értékelem.

A dolgozat következő jelentős kutatási eleme az ARDS-modell és az annak részét képező fájlkiszolgálói megoldás vizsgálata. A szerző olyan többretegű architektúrát mutat be, amely a monitorozást, a detektálást, az incidensválasz lehetőségét és a snapshot-alapú helyreállítást egyazon koncepcióban kapcsolja össze. Fontos eredménynek tartom, hogy a dolgozat a végleges változatban világosabban különíti el az ismert technológiák integrációját a saját tudományos és módszertani hozzájárulásoktól.

Külön értékelendő a heterogén kliens–szerver rendszerek teljesítményének összevetésére kialakított referencia-alapú relatív teljesítménymutató. A szerző nem egyszerűen az egyes konfigurációk abszolút átviteli sebességét hasonlítja össze, hanem olyan relatív mérési keretet alakít ki, amelyben az eltérő operációs rendszerek, fájlrendszerek és adatvédelmi mechanizmusok teljesítménye közös referencia alapján értékelhető.

A korábbi opponensi véleményben kérdésként merült fel a Windows Server 2019 referencia-környezet BitLocker és VSS nélküli alkalmazásának indokoltsága. A végleges értekezés erre megfelelő módszertani indoklást ad. A szerző a kevésbé terhelt Windows-konfiguráció alkalmazását konzervatív összehasonlítási alapnak tekinti, hiszen az ARDS-oldalon ezzel párhuzamosan ZFS-tükrözés, AES-256-GCM titkosítás és snapshot-kezelés is működik. Az összehasonlítás természetesen nem fedheti le a lehetséges vállalati konfigurációk teljes körét, de a választott vizsgálati elrendezés indokoltnak és tudományosan védhetőnek tekinthető.

Az értekezés legerősebb részének továbbra is a szerveroldali fájlműveleti naplókra alapuló gépi tanulási detekció vizsgálatát tartom. A szerző több mint 2,5 millió eredeti naplókorkorból kiindulva alakít ki előfeldolgozott, időablakokra aggregált adathalmazt, majd több klasszikus és ensemble gépi tanulási algoritmus – Random Forest, Support Vector Machine, Decision Tree, AdaBoost és XGBoost – teljesítményét hasonlítja össze. A modellek értékelése nem kizárólag pontosság alapján történik, hanem többek között érzékenység, specificitás, F1-, Precision–Recall-, ROC- és költségalapú szempontokat is figyelembe vesz.

A hiperparaméter-optimalizálást követően az XGBoost mutatta a legkedvezőbb összteljesítményt. A modell 0,919-es érzékenységet ért el, miközben az osztályozási idő a teljes, 392 időablakot tartalmazó teszt sor esetében is milliszekundumos nagyságrendben maradt. Ez megfelelő empirikus alapot biztosít a szerző azon következtetéséhez, hogy az alkalmazott feldolgozási módszer alkalmas lehet a zsarolóvírus-tevékenység kvázi valós idejű szerveroldali felismerésére.

Kifejezetten pozitívnak tartom, hogy a szerző a végleges dolgozatban már nem általánosítja indokolatlanul ezeket az eredményeket valamennyi zsarolóvírus-támadásra. Részletesen tárgyalja az intermittens, sparse, low-and-slow, partial és staged encryption technikákat, valamint a titkosítás nélküli zsarolás problémáját. Egyértelműen megállapítja, hogy a bemutatott modell elsősorban az intenzív fájlműveleti aktivitással járó, teljes titkosítást alkalmazó zsarolóvírusokra validált. Ugyancsak megfelelően jelenik meg a concept drift, a hosszú távú felhasználói viselkedésváltozás és az új ransomware-családokra történő általánosíthatóság kérdése mint további kutatási irány.

Az értekezés formai értékelése

Az értekezés szerkezete logikus, a kutatási folyamat jól követhető. A bevezető és módszertani részeket az empirikus vizsgálatok és a műszaki megvalósítás bemutatása követi, majd külön fejezetben jelennek meg a tézisek, az összegzés, a kutatás korlátai és a további kutatási lehetőségek.

A dolgozat ábra- és táblázatanyaga jelentős, alapvetően jól támogatja az eredmények megértését. A szakirodalmi háttér megfelelő, és a végleges változatban érzékelhetően erősebbé vált a korábbi munkákhoz történő kritikai viszonyítás.

A nyelvezet összességében megfelelő tudományos színvonalú és jól érthető. Helyenként továbbra is érzékelhető a mérnöki dokumentációs szemlélet, illetve egyes háttérmagyarázatok terjedelme nagyobb a feltétlenül szükségesnél, ez azonban a dolgozat értékelhetőségét nem befolyásolja.

Néhány terminológiai és szerkesztési pontatlanság is megmaradt. Ilyen például az ARDS rövidítés feloldásának nem mindenhol következetes használata (a dolgozat elején Anti-Ransomware Defense System, egy későbbi helyen viszont Autonomous Ransomware Detection System szerepel), valamint néhány kisebb nyelvi és tipográfiai hiba. Ezek javítása a végleges archivált változatban indokolt, de tudományos szempontból nem tekinthetők érdemi hiányosságnak.

A doktori tézisek értékelése

1. tézis

A szerző szerint a heterogén kliens–szerver architektúrák fájlátviteli teljesítménye páronként definiált, dinamikus referencia-alapú relatív teljesítménymutató segítségével objektíven összevethető.

A tézis világosan definiált módszertani eredményt fogalmaz meg. Külön érdeme, hogy a szerző az értekezés korábbi változatához képest elválasztotta ezt az eredményt az ARDS rendszer általános architektúrális kialakításától. A javasolt mutató alkalmazását empirikus mérésekkel demonstrálja, és az eredmény megfelelően általánosított formában jelenik meg.

Az 1. tézist új tudományos eredményként elfogadom.

2. tézis

A tézis szerint a centralizált fájlkiszolgáló környezetek szerveroldali, időbélyeggel ellátott fájlműveleti naplódadatai megfelelő előfeldolgozással és időablakos aggregációval olyan

strukturált idősoros reprezentációvá alakíthatók, amely kliensoldali információ nélkül is lehetőséget teremt intenzív fájlműveleti aktivitást generáló zsarolóvírusok kvázi valós idejű felismerésére.

A tézis megfelelően definiálja a módszer alkalmazási feltételeit és érvényességi tartományát. A szerveroldali, időablakos adatrepresentáció kialakítása önálló módszertani hozzájárulásként értékelhető, amely nem kötődik egyetlen konkrét gépi tanulási algoritmushoz.

Különösen fontosnak tartom, hogy a szerző a tézis alátámasztásakor explicit módon rögzíti a vizsgálat korlátait: a teljes titkosítást alkalmazó ransomware-eket, a centralizált fájlkiszolgálói környezetet és az intenzív fájlműveleti aktivitást.

A 2. tézist új tudományos eredményként elfogadom.

3. tézis

A szerző igazolja, hogy a normál felhasználói aktivitás és a vizsgált, teljes titkosítást alkalmazó zsarolóvírusok által generált intenzív fájlműveleti mintázatok bináris osztályozási problémaként kezelhetők, és megfelelő adatelőkészítés mellett klasszikus és ensemble gépi tanulási módszerekkel időkritikus döntési késleltetés mellett detektálhatók.

A tézist kiterjedt empirikus vizsgálat támasztja alá. A több modell összehasonlítása, a hiperparaméter-hangolás, a többféle értékelési metrika és a döntési késleltetés mérése együttesen megfelelő tudományos alapot biztosít az állításhoz.

A szerző itt is megfelelően lehatárolja az eredmények érvényességét, és nem terjeszti ki azokat a vizsgálatban nem szereplő, eltérő viselkedésű ransomware-típusokra.

A 3. tézist új tudományos eredményként elfogadom.

4. tézis

A szerző szerint a zsarolóvírus-detektálásra alkalmazott gépi tanulási modellek gyakorlati használhatóságának megítéléséhez egyetlen teljesítménymutató nem elegendő, és a pontosság, az F1-pontszám, az érzékenység, a specifitás, a keveredési mátrix és a költségalapú értékelés együttes alkalmazása biztosít megfelelő összehasonlítási alapot.

A tézisben megfogalmazott alapelv a gépi tanulási modellek értékelésének általános szakirodalmában ismert megközelítés, ezért önálló elméleti újdonságértéke az előző tézisekénél kisebb. A dolgozat eredménye ugyanakkor abban áll, hogy a szerző ezt a többkritériumos értékelési megközelítést a zsarolóvírus-detektálás speciális problémájára alkalmazza, és empirikusan igazolja, hogy a különböző hibák eltérő gyakorlati következményei miatt az egyes modellek sorrendje és alkalmazhatóságának megítélése egyetlen hagyományos teljesítménymutató alapján nem lenne kellően megalapozott.

Ezt alkalmazásspecifikus módszertani és validációs eredményként értékelve **a 4. tézist elfogadom.**

A jelölthöz intézett kérdések

1. A szerző a dolgozatban részletesen tárgyalja a concept drift problémáját és a modell rendszeres újratanításának lehetőségét. Egy ténylegesen üzemelő rendszer esetében milyen mechanizmust tartana alkalmasnak annak felismerésére, hogy a normál felhasználói viselkedés vagy a ransomware-ek működése olyan mértékben megváltozott, amely már a modell újratanítását teszi szükségessé?
2. A vizsgálat centralizált, virtualizált fájlkiszolgáló-infrastruktúrára vonatkozik. A szerző megítélése szerint mely részei vihetők át változtatás nélkül, illetve melyeket kellene alapvetően újragondolni felhőalapú vagy hibrid adattárolási környezetben?
3. A relatív teljesítménymutató alkalmazása szükségszerűen referencia-rendszer választását igényli. Hogyan befolyásolja a referencia megválasztása az eredmények értelmezését, és milyen szempontok alapján lehet egy általánosabb rendszer-összehasonlító vizsgálatban megfelelő referencia-konfigurációt kiválasztani?

Összegzés és javaslat

Arányi Gábor doktori értekezése aktuális, tudományosan és gyakorlatilag egyaránt releváns problémát vizsgál. A munka erőssége az empirikus és implementációs szemlélet, a heterogén informatikai környezetekben végzett teljesítményvizsgálat, valamint mindenekelőtt a szerveroldali fájlműveleti naplók viselkedésalapú, gépi tanulást alkalmazó feldolgozására kidolgozott módszer.

A végleges értekezésben a szerző megfelelően reagált a korábbi opponensi észrevételekre. Pontosította tudományos hozzájárulásait, átdolgozta és szűkebben definiálta téziseit, részletesen bemutatta a kutatás érvényességi korlátait, reflektált a modern zsarolóvírusok megváltozott működési mechanizmusaira, valamint egyértelműbbé tette eredményeinek tudományos pozicionálását.

Az értekezésben bemutatott kutatómunka terjedelme, módszertani megalapozottsága és eredményei véleményem szerint megfelelnek a doktori (PhD) fokozattal szemben támasztott követelményeknek. A megfogalmazott négy tézist elfogadom.

Mindezek alapján Arányi Gábor „Zsarolóvírus-támadások időkritikus felismerése gépi tanulás alkalmazási lehetőségeinek vizsgálatával centralizált fájl tárolási környezetekben” című értekezését elfogadásra javaslom, és alkalmasnak tartom arra, hogy a doktori (PhD) fokozat megadásának alapjául szolgáljon.

Budapest, 2026. augusztus 17.



Dr. Krasznay Csaba

habilitált egyetemi docens

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék