
Doktori értekezés bírálata

A jelölt neve: Arányi Gábor

Az értekezés címe: Zsarolóvírus-támadások időkritikus felismerése gépi tanulás alkalmazási lehetőségeinek vizsgálatával centralizált fájl tárolási környezetekben

A bíráló neve és tudományos fokozata: Kő Andrea, PhD

Arányi Gábor kutatásának elsődleges célja egy olyan gyakorlatban is alkalmazható védelmi modell kidolgozása volt, amely a centralizáltan tárolt adatvagyon védelmére szolgál és képes a zsarolóvírus-támadás időkritikus felismerésére. A dolgozat fő eredménye az ARDS (Anti-Ransomware Defense System) koncepcionális modell kidolgozása, valamint a modell részét képező fájl kiszolgáló oldali védelmi megoldás gyakorlati alkalmazhatóságának igazolása referenciaalapú teljesítményértékeléssel.

A disszertáció tartalmazza a következő részterületeket:

- a vonatkozó szakirodalom áttekintése;
- a tudományos probléma megfogalmazása;
- a kutatási célok és kutatási módszerek megfogalmazása;
- fejezetenként az elvégzett vizsgálatok és a részkövetkeztetések leírása;
- a következtetések összefoglalása;
- az új tudományos eredmény(ek) megfogalmazása;
- a hivatkozott irodalom listája;
- a doktorandusz témával kapcsolatos publikációs listája.

Az értekezés tartalma megfelel az alábbi követelményeknek:

- új tudományos eredményeket tartalmaz;
- bizonyítja, hogy a Jelölt önálló problémafeltáró, kísérletező, elemző, alkalmas kreatív kutatómunkára,
- a dolgozathoz kapcsolódóan a Jelölt alapos ismeretekkel rendelkezik a témában, és képes azt kreatívan felhasználni,
- a téma logikusan és átláthatóan van bemutatva, a kutatási terület korszerű szinten kerül ismertetésre;
- az értekezés tartalma megfelel a tudományos írási és tartalmi követelményeknek;
- az értekezés összefoglalja és értékeli a kutatási témához kapcsolódó szakirodalmat;
- a kutatási célok bemutatása, a kutatási módszerek és eredmények bemutatása megtörténik;
- a gyakorlati alkalmazási lehetőségek bemutatása kifejtésre kerül;
- a Jelölt bemutatja az önálló egyedi következtetéseket és az új tudományos eredményeket;
- az értekezés szöveges részét a választott kutatási témához illeszkedő mellékletek, valamint a Jelölt által publikált publikációk listája egészíti ki;
- a megvalósult munka tudományos módszerek alkalmazásának bizonyított eredménye - kidolgozása önálló alkotó tevékenységet bizonyít;
- az eredmények kielégítik a kutatási terület gyakorlati alkalmazásával kapcsolatos igényeket.

RÉSZLETES MEGJEGYZÉSEK

A disszertáció témaválasztásának elméleti és gyakorlati jelentőségét, valamint aktualitását az is alátámasztja, hogy a zsarolóvírus-támadások az utóbbi években az informatikai rendszereket érintő egyik legsúlyosabb és legdinamikusabban terjedő fenyegetéssé váltak. Ez különösen igaz a kis- és középvállalkozások (KKV-k) körére, ahol a védekezés lehetőségei gyakran mind pénzügyi, mind szakmai szempontból korlátozottak.

A disszertáció nyolc fejezetből áll, a szerző az opponensi visszajelzések alapján szerkezeti módosításokat végzett. Új a kutatómódszertani fejezet, valamint több fejezet átstrukturálása is megtörtént, így a kutatás logikai folyamatához jobban illeszkedő tartalom jött létre.

A bevezetésben a szerző áttekinti a zsarolóvírus-támadások aktuális trendjeit és gazdasági hatásait, majd összefoglalja a leggyakoribb támadási formákat és a leginkább érintett szektorokat. Ismerteti a kutatás háttérét és motivációját, meghatározza a célkitűzéseket, valamint felvázolja a várható eredményeket. Az 1.6 fejezetben bemutatja eddigi publikációs tevékenységét és hivatkozási mutatóit.

A második fejezet módszertani áttekintést ad, kitérve a szakirodalom elemzésére, a kérdőíves kutatásra, valamint a mesterséges intelligencia eszközeinek kiválasztására.

A kiválasztott módszertani megközelítések relevánsak. A szakirodalom feldolgozásnál a napjainkban leggyakrabban alkalmazott PRISMA megközelítést használja a szerző. A tervezethez képest, a szerző pontosította a leírást a PRISMA módszerről, a kérdőíves kutatás módszertanáról, valamint a gépi tanulási modellek kiválasztásának indoklásáról. Frissítette a szakirodalmi áttekintést a 2025–2026-ban megjelent nemzetközi kutatásokra és iparági riportokra fókuszálva. A kérdőíves vizsgálat esetében kiegészítette a mintavétel indoklását, a kutatás korlátainak ismertetését, valamint az eredmények értelmezését.

A kérdőívet 46 vállalat töltötte ki, amelyeket célzott (purposive) megközelítéssel választott ki a szerző. A mintában szereplő vállalatok részletesebb bemutatása a 4.3 fejezetben történik meg, a módszertani leírásban annyit tudunk meg a célcsoportról, hogy magyarországi kis- és középvállalkozások, amelyek működésük során informatikai rendszereket, digitális adatvagyonot és hálózati infrastruktúrát használnak. A szerző szakmai kapcsolatrendszerét felhasználva olyan vállalatokat választott be a mintába, amelyek esetében az informatikai üzemeltetés jellemzően saját erőforrásokra vagy kis létszámú külső szolgáltatóra támaszkodik.

A kutatási folyamat vizualizációjára vonatkozó 7. ábra inkább ehhez a fejezethez illeszkedik, mint a negyedik, kérdőíves felmérést tárgyaló fejezethez.

A szakirodalom áttekintéssel több fejezet foglalkozik. Egyrészt a harmadik fejezet, bár ez rövid, két oldal, de az 5.1 fejezet (adatvagyon védelmét és visszaállíthatóságát biztosító kísérleti megoldások), és a 6.1-es fejezet (a zsarolóvírusok észlelésére, a honeypot-alapú megoldásokra fókuszál) is tartalmaz szakirodalomfeldolgozáshoz köthető részeket.

A negyedik fejezet mutatja be a hazai kis- és középvállalkozások körében végzett informatikai biztonságra fókuszáló kérdőíves felmérés eredményeit, majd ismerteti az ARDS védelmi modellt. Továbbra sem derül ki a dolgozatból, hogy a kérdőíves felmérés célcsoportjának meghatározásakor mennyire volt meghatározó szempont a működési terület. A disszertáció felsorolja, hogy a célcsoport ilyen szempontból heterogén, de a kiválasztási

szempontok között ez nem szerepel, pedig vannak olyan működési területek, amelyek esetében az informatikai védelmi tudatosság szintje valószínűsíthetően magasabb.

A mintában a 8. ábra alapján 23 mikrovállalkozás van, de az ő válaszaik nincsenek elkülönítve a nem mikrovállalkozási válaszoktól. Ezt érdemes lett volna megtenni, mert a méret is jelentős befolyásoló tényező lehet. A kutatásnak ez a része feltáró jellegű.

Az alábbi állítást érdemes lett volna pontosabban megfogalmazni: „a megkérdezett vállalkozások nagy része 2020 áprilisa és 2021 márciusa között valamilyen rosszindulatú szoftveres támadás, egyes esetekben zsarolóprogram áldozata lett.”, mivel a disszertáció a zsarolóvírusokra fókuszál.

A 4.4 rész (az eredmények összefoglalása, releváns kutatási kérdések megválaszolása) 6. táblázatának (Az otthoni munkavégzés és a zsarolóvírus-támadások közötti összefüggés) soraiban milyen változók szerepelnek?

A 4.5 fejezet ismerteti a disszertáció fő eredményének számító ARDS modellt, bemutatás kellően részletes, jól követhető.

Az ötödik fejezet az ARDS modell fájlkezelőjének teljesítményértékelését részletezi. Az eredmények meggyőzőek és jól hasznosíthatók.

Az hatodik fejezetben a zsarolóvírus-támadások felismerésének lehetőségét vizsgálja a jelölt fájlműveleti naplófájlok alapján, gépi tanulási modellek segítségével. Az opponensi visszajelzések alapján ebben a fejezetben a szerző bővítette az előfeldolgozás, a modellkiválasztás, a hiperparaméter-hangolás, a statisztikai validálás, valamint a költségalapú értékelés bemutatását. A javasolt megközelítés erősségeit és korlátait a 20. táblázat foglalja össze. A megállapításokkal egyetértek, a megközelítés egyik fő korlátja a kellően reprezentatív tanítási adathalmaztól való függőség, ugyanakkor az ARDS modell egy hatékony megoldási alternatíva lehet.

A hetedik fejezet ismerteti a doktori értekezés téziseit, az azokhoz kapcsolódó eredményeket, valamint a tézisek igazolásához köthető publikációkat.

Az első tézist és annak alátámasztását a heterogén kliens–szerver architektúrák fájlátviteli teljesítményéről elfogadom új tudományos eredményként.

A második tézist és annak alátámasztását a strukturált idősoros reprezentáció kialakításáról és alkalmazhatóságáról elfogadom új tudományos eredményként.

A harmadik tézist és annak alátámasztását a gépi tanulási modellek alkalmazhatóságáról elfogadom új tudományos eredményként.

A negyedik tézist és annak alátámasztását a gépi tanulási modellek értékeléséről elfogadom új tudományos eredményként.

A záró, nyolcadik fejezet összegzi az eredmények tudományos jelentőségét, bemutatja azok korlátait és értelmezési szempontjait, továbbá kijelöli a jövőbeli kutatási irányokat és feladatokat.

Összegezve, a választott kutatási téma fontos és időszerű, a disszertációban tárgyalt kutatási problémák tudományos jelentőségűek. A kutatás céljai, alkalmazott módszerei és elért eredményei egymással összhangban állnak, és konzisztens egész alkotnak.

A disszertációtervezetre adott bírálatok alapján a szerző lényeges, valamennyi felvetésre kiterjedő átdolgozást végzett és a felmerült kérdésekre is válaszolt.

Az értekezés nyilvános védésre bocsátását támogatom, sikeres védés esetén a fokozat odaítélését javaslom.

Kérdések:

Milyen módosításokra lenne szükség az ötödik fejezetben ismertetett mérés megismétléséhez, ha az újabb Windows Server verziókat (Windows Server 2022, vagy Windows Server 2025) vennénk figyelembe a Windows Server 2019 helyett?

Kellene-e módosítani az ARDS fogalmi modellen egy ilyen esetben és ha igen mit?

Budapest, 2026. szeptember 25.



Andrea Kő, Ph.D., CISA
Director, Institute of Data Analytics and Information
Systems
Professor, Corvinus University of Budapest
H-1093 Fővám tér 13-15.
Budapest, Hungary
Tel: +36-1-482-7416
e-mail: andrea.ko@uni-corvinus.hu