Lehrer Zoltán

Az alábbi opponensi értékelést **az opponensi bírálati lap logikája** és a megadott **pontmaximumok** szerint készítettem.

> **Megjegyzés (plágium/AI):** valódi plágiumvizsgálatot (adatbázisok, Turnitin stb.) innen nem tudok futtatni; ezért **szöveg- és hivatkozás-alapú gyanújelzéseket** adok, illetve javaslom az intézményi eszközzel történő ellenőrzést.

---

0) Plágiumgyanú és AI-használat (minőségi megállapítás)

Pozitívumok

- A szerző **explicit módon deklarálja a ChatGPT használatát**, és azt is állítja, hogy a válaszokat ellenőrizte, illetve saját gondolatokkal egészítette ki.
- A dolgozat **külön mellékletben** utal „releváns LLM konverzációk teljes szövegére”, ami transzparenciát erősít.
- A munka több helyen **saját fejlesztést** (C# konzolalkalmazás, ML.NET modell) és módszertani elemeket (log-alapú elemzés, COCO Y0/OAM) hangsúlyoz.

Kockázati/gyanújelek (nem bizonyítékok)

- A szakirodalmi fejezetben több rész **tankönyvszerű, generikus megfogalmazású** (pl. tantárgyak “mit adtak” jellegű leírásai), ami AI-szövegre is hasonlíthat – de önmagában nem plágium.
- Néhány hivatkozásnál érdemes lenne **forrásminőség/ellenőrizhetőség** audit (pl. pontosság, kiadó, URL-archiválás hiánya szerepel is mint korlát).

Összegzés: plágiumgyanú érdemben nem állapítható meg pusztán a szöveg

alapján; az AI-használat **deklarált és dokumentált**, ami kifejezetten jó gyakorlat.

---

1) Téma és célkitűzések — 38 / 40

Erősségek

- A téma aktuális és releváns: **USB háttértárak kockázatelemzése**, log-alapú sérülékenységi szemlélet, AI/ML alkalmazás.
- A célok több szinten meg vannak fogalmazva: módszertan + prototípus jellegű megvalósítás (COCO Y0 + ML.NET + C# alkalmazás), célcsoportok is szerepelnek.

Fejlesztendő

- A célok „üzleti hasznosság" része (idő/költség) erős, de a **kutatási kérdés/hipotézis** és a **mérési siker-kritériumok** (pl. pontosság, téves riasztás) még explicitálhatóbb lenne.

---

2) Szakirodalom feldolgozása — 36 / 40

Erősségek

- Széles spektrum: IT-biztonsági keretek (pl. szabványok/irányelvek említése), jogi háttér (GDPR), USB-technikai alapok (pl. „magic number"), módszertani kitekintés.
- Van törekvés összehasonlításra és kontextusba helyezésre (más COCO-alapú megközelítések említése).

Fejlesztendő

- A szakirodalom egy része **tananyagi jellegű**, kevésbé kritikai-szintetizáló. (Mit mondanak a források? Miben vitatkoznak? Mi a "gap"?)
- Jó lenne egységesebb, auditálhatóbb hivatkozási apparátus (bibliográfiai teljesség, URL-archiválás, elsődleges vs. másodlagos források elkülönítése).

---

3) A szerző saját munkájának bemutatása — 55 / 60

Erősségek

- Egyértelműen megjelenik a **saját fejlesztésű C#/.NET konzolalkalmazás** és az **ML.NET-alapú osztályozó modell** ötlete; a fájl-jellemzők (pl. méret, entrópia) alapú kockázatbecslés koncepciója érthető.
- A dolgozat reflektál a megoldás korlátaira (statikus elemzés, korlátozott adathalmaz, valós idejű védelem hiánya, teljes körű audit hiánya). Ez szakmai érettséget mutat.
- AI/LLM szerepének elkülönítése (támogató, nem helyettesítő) és a dokumentálás említése szintén plusz.

Fejlesztendő (amiért nem 60)

- A „saját munka” legerősebbé tétele érdekében hiányzik/kevésbé hangsúlyos a **kvantitatív értékelés**: tanító/teszt adathalmaz jellemzése, metrikák (accuracy, precision/recall, F1, ROC-AUC), konfúziós mátrix, baseline összevetés.
- A biztonsági eszköz jelleg miatt hasznos lenne egy rövid **fenyegetési modell** (threat model) és „false positive/false negative” kezelési stratégia.

---

4) Szerkezet, stílus és formai szempontok — 36 / 40

Erősségek

- Strukturált, fejezetek hierarchikusan, mellékletek (rövidítések, definíciók, hivatkozások, ábra- és táblázatjegyzék) említettek.
- Tudatos formai hivatkozás az intézményi mintára/struktúrára; követhető felépítés.

Fejlesztendő

- Stílusban időnként **ismétlő, tananyagos** részek; feszesebb szerkesztéssel

rövidíthető lenne.

- Hivatkozások/online források archiválása nem történt (a dolgozat maga jelzi), ez opponensi szempontból formai-könyvészeti kockázat.

---

5) Összbenyomás — 18 / 20

Összkép

- **Innovatív és gyakorlatias** téma; jó transzparencia AI-használatban; a saját fejlesztés iránya meggyőző.
- A "proof-of-concept" jelleg vállalható, de a tudományos erőt a **mérhető eredmények** és validáció még tovább növelné.

Pontösszesítés és érdemjegy-javaslat

- Téma és célkitűzések: **38 / 40**
- Szakirodalom feldolgozása: **36 / 40**
- Saját munka: **55 / 60**
- Szerkezet/stílus/forma: **36 / 40**
- Összbenyomás: **18 / 20**

Összesen: 183 / 200 pont → „Kiváló" (180–200)

Rövid, beírható „Általános összefoglaló vélemény" (opponensi lapra)

- **Téma és célkitűzések:** aktuális, jól körülhatárolt, gyakorlati haszonnal; a siker-kritériumok még mérhetőbben definiálhatók.
- **Szakirodalom:** széles körű, releváns; több kritikai szintézis és forrás-audit erősítené.
- **Saját munka:** meggyőző prototípus-szemlélet (C# + ML.NET + log-alapú

megközelítés); kvantitatív validáció bővíthető.

- **Szerkezet/stílus/forma:** jól tagolt, mellékletek és segédelemek; tömörítés és hivatkozás-egységesítés javasolt.
- **Összbenyomás:** érett, modern, transzparens AI-használat; további mérésekkel publikálhatóbb szintre emelhető.

Védésre javasolt kérdések (3 db)

1. Milyen metrikákkal igazolná a modell használhatóságát (precision/recall, F1, ROC-AUC), és mi lenne az elfogadható téves riasztási ráta?
2. Mi a legfontosabb „adatszivárgási" vagy „fertőzési" fenyegetési forgatókönyv USB-ről, és hol illeszkedik ebbe a prototípus?
3. Hogyan bővítené a statikus elemzést dinamikus sandbox/viselkedéselemzéssel, és milyen erőforrás-korlátokkal számolna?

Ha szeretnéd, a következő lépésként **kitöltöm szövegszerűen az opponensi lap üres mezőit** (pontok + rövid indoklások + összefoglaló), hogy egy az egyben bemásolható legyen.