Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Student: **Bc. Jan Zdražil** **Vedoucí práce:** **Ing. Milan Oulehla, Ph.D.**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2022/2023**

Téma diplomové práce: **Detekce malwaru běžícího pod operačním systémem Android s využitím metod strojového učení**

Hodnocení práce:		**A**	**B**	**C**	**D**	**E**	**F**
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Splnění všech bodů zadání	☒	☐	☐	☐	☐	☐
2.	Vhodnost zvolené metody řešení	☒	☐	☐	☐	☐	☐
3.	Členění práce (kapitoly, podkapitoly, odstavce)	☐	☒	☐	☐	☐	☐
4.	Práce s literaturou a její citace	☒	☐	☐	☐	☐	☐
5.	Úroveň jazykového zpracování	☒	☐	☐	☐	☐	☐
6.	Formální úroveň práce	☐	☒	☐	☐	☐	☐
7.	Kvalita zpracování teoretické části	☒	☐	☐	☐	☐	☐
8.	Kvalita zpracování praktické části	☒	☐	☐	☐	☐	☐
9.	Dosažené výsledky práce	☒	☐	☐	☐	☐	☐
10.	Přínos práce a její využití	☒	☐	☐	☐	☐	☐
11.	Spolupráce autora s vedoucím práce	☒	☐	☐	☐	☐	☐

Výsledek kontroly plagiátorství:
Práce byla posouzena z hlediska plagiátorství s výsledkem 3% shodnosti. Práce není plagiát.

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Vypracování diplomové práce bylo příkladné. Student pravidelně konzultoval zpracování jednotlivých částí závěrečné práce a připomínky vedoucího práce systematicky zapracovával.

Práce vychází z nejnovějších poznatků v oblasti detekce mobilního malwaru, které využívají metod umělé inteligence. Zajímavé je například použití transformátorů.

Obvyklý postup detekce mobilního malwaru je založený na extrakci charakteristik, jako jsou oprávnění, API volání apod. Tato práce však využívá moderní, méně používaný postup založený na zpracování obrazu, který převádí data jednotlivých vzorků (APK balíčků) a jejich částí do obrazové podoby. Na takto získaná obrazová data pak byly aplikovány metody strojového učení.

Nejdůležitějšími výsledky diplomové práce jsou:
- modely, které byly vytvořeny přímo pro potřeby detekce mobilního malwaru: Malware Detection-Neural Network Model (MD-NNM) a Malware Detection-Vision Transformer Neural Network Model (MD-ViTNNM),
- porovnání vytvořených modelů MD-NNM a MD-ViTNNM s moderními modely DenseNet a ResNet. Výsledky srovnání ukázaly, že vytvořené modely dosahovaly lepších detekčních výsledků.

V práci byly také adekvátním způsobem popsány omezení související s výpočetním výkonem a počtem vzorků.

Celkově se jedná o zdařilou diplomovou práci, o čemž svědčí i následující skutečnosti:
- vysoká přesnost detekce vzorků malwaru (neznámá data),
- třetí místo v soutěži STOČ,
- vytvořené modely MD-NNM, MD-ViTNNM a soubory obrazových dat, kterou budou využívány v navazujícím výzkumech v PT LAB při UTB.

Datum 1. 6. 2023 Podpis vedoucího diplomové práce