FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Simona Fornůsek, Ph.D.
Student:	Bc. Jaroslav Pešek
Název práce:	Framework pro automatické zlepšování klasifikace síťového provozu
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	29. května 2022

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Dle zadání měl autor vytvořit softwarový prototyp frameworku pro automatické vyhodnocování a vylepšování výsledků algoritmů strojového učení pro klasifikaci síťového provozu a detekci bezpečnostních hrozeb, seznámit se s problematikou klasifikace síťového provozu pomocí IP Flows a prozkoumat problematiku vyhodnocování přesnosti klasifikátorů v laboratorních podmínkách a při reálném nasazení a automatického vylepšování datových sad (např. pomocí Active Learning).

Všechny body ze zadání jsou v práci obsaženy a splněny.

2. Písemná část práce 90 /100 (A)

Text práce je dobře strukturovaný a čtivý, pokrývá veškeré aspekty ze zadání, rešeršní i implementační část je obsahově bohatá a kvalitně zpracovaná.

3. Nepísemná část, přílohy 90 /100 (A)

Nepísemnou část práce tvoří zdrojové kódy prototypu a skriptů z testování, což považuji za adekvátní. Orientaci v kódu by ulehčili chybějící komentáře.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Jelikož má implementační část práce formu modulu do již stávajícího systému NEMEA, zajisté najde praktického využití - jak autor zmiňuje v práci, plánuje se nasazení

vyvinutého frameworku v síti CESNET. Práce rovněž v závěru ukazuje na možné další směry rozšíření a dalšího výzkumu.

Celkové hodnocení

90 /100 (A)

Vzhledem ke kvalitnímu zpracování tématu práci doporučuji k obhajobě, a hodnocení stupněm "A".

Otázky k obhajobě

V práci zmiňujete kratší výpadky v průběhu testování, způsobeny neodladěnými chybami - jaké to byly chyby, a jak jste se s nimi vypořádal?
V čem spatřujete hlavní přínosy Active Learning pro detekci bezpečnostních hrozeb v síťovém provozu? Má tato metoda i potenciální slabiny?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.