FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Olha Jurečková
Student:	Bc. Vojtěch Skalák
Název práce:	Klasifikace malwaru na základě samoorganizačních map
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	29. května 2024

Hodnotící kritéria

1. Splnění zadání

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

Zadání považuji za splněné, ale s velkými výhradami. Text práce obsahuje překlepy, chyby ve formátování a experimenty nejsou dostatečně popsány. Kap. 3.2 „Malware classification results" je příliš krátká – o trochu víc než jedna stránka. Hyperparameter tunning algoritmu SOM nebyl proveden dostatečně dobře, což mělo za následek horší klasifikační výsledky.

2. Písemná část práce 50 / 100 (E)

Text práce obsahuje následující nedostatky. Popis PE formátu i algoritmu SOM nepatří do "Introduction". Do první kapitoly "Literature review" nepatří seznam datasetů a naopak tam mohlo být zmíněno více článků, kde se využil algoritmus SOM pro klasifikaci malwaru. Z kapitoly 2 není jasné, jestli student implementoval SOM algoritmus sám, nebo ji převzal z existující knihovny. Největším nedostatkem práce je kapitola 3 "Results". Uvádím zde jenom některé komentáře:
- str. 21: v kap. 3.1.1. o PCA chybí vysvětlení notace použité v krocích 1. až 4.
- str. 22: v kap. 3.1.1. o PCA není přesně popsáno, proč se vybrala hodnota 20 z tab. 3.1. Proč se např. nevybralo 50 příznaků, pro které se dosáhla nejvyšší přesnost? Taky není napsáno, jestli výsledky z tab. 3.1. jsou pro detekci malwaru, nebo klasifikaci malwaru do rodin. Navíc nejsou specifikovány hyperparametry SOMu.
- str. 23: v kap. 3.1.2.2 se uvádí "The results in the table 3.3 suggest that the combination with the best performance is 100 iterations and 0.01 learning rate." avšak tab. 3.3 takovou kombinaci neobsahuje. Nejvyšší přesnost byla dosažena pro počet iterací 1000 a learning rate 0.001. Také nejsou specifikovány ostatní hyperparametry SOMu.
- student neaplikoval hyperparameter tunnig na všechny hyperparametry spolu, ale

naopak na některé hyperparametry (např. "Size of the map") aplikoval hyperparameter tunning nezávisle na ostatních hyperparametrech.
- obrázky 3.1 až 3.4 a také několik tabulek (3.10 nebo 3,11) výrazně zasahují přes okraj. Navíc obrázky i tabulky jsou nesprávně umístněny.
- u MLP proběhl hyperparameter tunning jenom pro skryté vrstvy a není uvedeno, s jakými počty neuronů se experimentovalo.

Student výsledky experimentů s vedoucí diplomové práce vůbec nekonzultoval, což vedlo k několika chybám a nedostatečnému vysvětlení.
Chybí závěr práce. Je uvedena pouze krátká diskuze o experimentálních výsledcích.

3. Nepísemná část, přílohy

45 /100 (F)

Nepísemná část diplomové práce se zdá být neúplná. Experimentální výsledky nelze ověřit, protože zdrojové kódy nejsou kompletní. Např. soubor som.py obsahuje přípravu validační sady pro hyperparameter tunning, ale vůbec se k tomu nepoužívá. Nepodařilo se mi najít zdrojové kódy pro experimenty s klasifikátory MLP a KNN.

4. Hodnocení výsledků, jejich využitelnost

45 /100 (F)

Protože pro algoritmus SOM nebyl dostatečne dobře vykonán hyperparameter tunning, student nedosáhl dobrých výsledků, kterých by potenciálně mohl dosáhnout. Z tohoto důvodu je využitelnost výsledků nízká. Text práce obsahuje poměrně podrobný popis algoritmu SOM, který může pomoci k lepšímu pochopení tohoto algoritmu a jeho následné implementaci.

5. Aktivita studenta

[1] výborná aktivita
[2] velmi dobrá aktivita
▸ **[3] průměrná aktivita**
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Aktivita studentu byla průměrná. Studentovi někdy trvalo několik dní, než odpověděl na dotazy.

6. Samostatnost studenta

[1] výborná samostatnost
[2] velmi dobrá samostatnost
▸ **[3] průměrná samostatnost**
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Samostatnost studenta byla průměrná. Na konzultacích jsme často řešili i jiné věci, než které se pak student rozhodl zařadit do práce.

Celkové hodnocení

50 /100 (E)

Student podrobně zpracoval algoritmus SOM, který byl jádrem jeho diplomové práce. Experimentální část je však slabší a příliš krátká. Finální verzi textu jsem obdržela den před odevzdáním, což mělo za důsledek, že práce nebyla zkontrolována. Z výše uvedených důvodů hodnotím práci známkou E na nejnižší možné hranici přijatelnosti.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.