FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Eliška Krátká
Název práce:	Metody kvantového počítání pro klasifikaci malware
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	3. června 2024

Hodnotící kritéria

1. Splnění zadání

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

Všechny body ze zadání práce považuji za splněné.

2. Písemná část práce 92 /100 (A)

Práce je dobře členěná, má odpovídající rozsah a seznam literatury obsahuje jen relevantní práce. Na začátku je čtenář obeznámen s problematikou detekce malwaru pomocí strojového učení se zaměřením na algoritmus SVM a jeho verzi pro kvantové počítání, která je naimplementována a aplikována na předzpracovaný veřejně dostupný dataset. Experimentální část mohla být detailněji popsána a mohlo být provedeno více experimentů. Např. informace o tom, že vzorky z datasetu byly vybrány náhodně a tak, aby počty v obou třídách byly zhruba stejné, se vyskytla až v kapitole 4.5 Discussion. Také odborníci pod výrazem "malware classification" chápou klasifikaci malwaru do rodin a ne detekci malwaru, čemuž se věnovala tato práce. Dále uvádím ještě některé drobné nedostatky:
- seznam zkratek není kompletní (chybí zkratky jako PE, DLL nebo COFF)
- v textu se vyskytuje pojem "klasické algoritmy". Z kontextu se dá pochopit, že se nejedná o kvantové algoritmy, ale bylo by dobré to explicitně uvést
- v textu se několikrát zavádí stejná zkratka, např. QSVM až 9krát
- názvy tříd na stř. 26 a 27 výrazně zasahují za okraj
- virtuální stroj z CloudFIT není specifikován
- tabulka 4.7 se mohla o trochu zmenšit a přesunout se na stranu 38 pod tabulku 3.6
Nakonec oceňuji, že v práci je detailně specifikována uživatelská dokumentace k programům provádějícím experimentální část.

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

Studentka si dala záležet na nepísemné části. Vyřešila několik technických problémů a připravila a zdokumentovala skripty pro další použití v navazujících pracích. Naměřené výsledky lze ověřit pomocí přiložených skriptů a veřejně dostupného datasetu.

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

Celá práce je podle mého názoru až příliš ovlivněna článkem „Quantum Machine Learning for Malware Classification" [12], který však v době psaní práce a tohoto posudku nebyl recenzován a obsahuje některé nedostatky v experimentální části, které jsou převzaty i v diplomové práci. Protože se však studentka rozhodla pokračovat v této práci v rámci doktorského studia, tak můžeme očekávat, že svou práci výrazněji rozšíří.

Celkové hodnocení 94/100 (A)

Studentka prokázala schopnost nastudovat si poměrně náročnou problematiku a vyřešit řadu technických problémů, aby dosáhla experimentálních výsledků na kvantovém počítači. Problematiku kvantového počítání pro detekci malwaru pěkně zpracovala do textu a připravila skripty s podrobnou dokumentací k dalšímu použití. Z těchto důvodů navrhuji známku A - výborně.

Otázky k obhajobě

1. Mohla by studentka detailněji vysvětlit vztah (2.7) na straně 16?
2. Velikosti trénovacích a testovacích sad z tabulek 4.1 až 4.4 jsou převzaty z článku [12], kde jsou však uvedeny výsledky i pro větší sady (konkrétně pro trénovací sadu velikosti 16 000 a testovací sadu velikosti 4 000). Proč pro tuto a ještě větší sady nebyly provedeny experimenty? Jaké byly výpočetní časy pro tyto tabulky?
3. Proč se pro IBM kvantový počítač využívaly tak malé trénovací a testovací sady? Experimenty začínají s trénovací sadou velikosti 4 a testovací sadou velikosti 2. Má smysl používat takto malé sady?
4. Proč se binárky převedly právě na obrázky a jakým způsobem se zvolila velikost obrázků? Nemůže útočník použitý způsob převedení na obrázky jednoduše zneužít tak, aby SVM, resp. QSVM, dosahovaly nízkých přesností detekce malwaru?

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.