POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Anomaly Detection in Threat Intelligence Data**
Jméno autora:	**Petr Marek**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	Mikuláš Krupička
Pracoviště oponenta práce:	Katedra teoretické informatiky, FIT ČVUT

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — náročnější

Hodnocení náročnosti zadání závěrečné práce.

Cílem práce bylo jak nastudovat a pochopit problematiku detekce hrozeb ve bezpečnostních datech, tak navrhnout a implementovat zlepšení těchto algoritmů včetně jejich praktickému použití na reálných datech. Vzhledem k množství kroků, které student musel zkombinovat, hodnotím zadání jako náročnější.

Splnění zadání — splněno s menšími výhradam

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání bylo splněno s některými menšími výhradami uvedenými dále v textu. Tyto se týkají především formální úrovně práce.

Zvolený postup řešení — správný

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student zvolil postup adekvátní zadání. Práce začíná teoretickým úvodem popisujícím problematiku a jednotlivé přístupy k řešení. Dále student jeden vybírá a rozšiřuje jej. Pak diskutuje způsob vyhodnocení a aplikuje jej na prezentovaný model. Místy postrádám podrobnější zdůvodnění jednotlivých kroků (např. právě odůvodnění volby výchozího modelu by mohlo být širší). Celkově je však práce dobře vedena.

Odborná úroveň — B - velmi dobře

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Odborná úroveň práce je zdařilá. Student se seznámil a pochopil problematiku časových řad, jejich modelování a detekce anomálií na nich. Vyhodnocení výsledků by mohlo být rozsáhlejší, především porovnání s jinými metodami. Nicméně samotnou problematiku vyhodnocení student diskutuje dostatečně.

Formální a jazyková úroveň, rozsah práce — D - uspokojivě

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

V jazykové úrovni práce jsem výraznější chyby nenalezl. Svým rozsahem patří práce spíše ke kratším, především teoretická část by mohla být rozsáhlejší. Bohužel ve všech grafech chybí jakékoli popisky os. Stejně tak na grafy je odkazováno jen nepřímo („druhý graf v této kapitole“), student vůbec nevyužil možnost jejich referencí. Kapitoly jsou však referencovány hojně. V práci jsem nenašel způsob výpočtu „seasonal influences“ grafu. Vzhledem k množství rovnic by se v práci hodilo uvést seznam použitých zkratek a značení.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Výběr zdrojů, korektnost citací	C - dobře

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Vzhledem k použitému typografickému systému LateX neshledávám ve formální stránce citací žádné problémy. V teoretickém úvodu je množství citací dostatečné, ve zbytku textu by však mohly být hojnější. V práci jsou místy části textu uvedeny bez jakékoli citace (např. na stranách 13, 15, 24). Čtenář je tak ponechán úvahám odkud student čerpal, případně co ho vedlo ke zvolenému kroku. U citací rozsáhlejších publikací by také bylo vhodné uvést přesnější citaci než publikaci samotnou (např. včetně kapitoly). Vlastní přínos by v práci mohl být prezentován výrazněji. To je pravděpodobně způsobeno členěním textu, kdy kromě State of the Art kapitoly je čtenář seznamován s teorií v průběhu celé práce. Nicméně v úvodu práce student seznamuje čtenáře se splněním zadání dostatečně (a odkazuje ho na příslušné části textu).

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Výsledky jsou v práci prezentovány dostatečně. Zdojový kód je vysvětlen dostatečně, ale na přiloženém CD chybí data, která student použil pro vyhodnocení. K samotnému paralelnímu zpracování dat je sice zmíněno, že nebylo cílem této práce nicméně i tak by bylo vhodné uvést podrobnější vysvětlení napojení na použitou architekturu.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Práce je dobře teoreticky zvládnuta. Výsledky jsou prezentovány dostatečně a zadání splněno v plném rozsahu. Největší nedostatek práce spatřuji v její formální části a práci se zdroji, jak je vysvětleno v příslušných sekcích. A vzhledem k náročnějšímu zadání tak hodnotím práci stupněm B.

Otázky:

- Zadání v bodě 5 se týká zpracování dat a zmiňuje se o rozšíření pipeline. Došlo k němu nějakým způsobem?
- Dokázal by prezentovaný model postihnout i troj-sezónní (a více) data?
- Jak se model dokáže vypořádat s více výpadky v rámci jedné řady?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm B - velmi dobře.

Datum:

Podpis: