OPONENTNÍ POSUDEK DOKTORSKÉ DISERTAČNÍ PRÁCE

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Obor: Inženýrská informatika

Téma disertační práce:	Návrh a ověření detekce systému anomálií založeného na strojovém učení v průmyslových řídících systémech
Autor práce:	Ing. Jan Vávra
Vypracováno na pracovišti:	Ústav bezpečnostního inženýrství
Studijní program:	Inženýrská informatika
Vedoucí disertační práce:	doc. Ing. Luděk Lukáš, Ph.D.
Konzultant:	doc. Ing. Martin Hromada, Ph.D.

Aktuálnost tématu disertační práce

Předložená disertační práce je věnována tématu detekce anomálií založeného na strojovém učení v průmyslových řídicích systémech. **Téma je významné**, aktuální a na pracovištích Fakulty aplikované informatiky řešitelné.

Splnění stanovených cílů v disertační práci

Autor stanovuje hlavní cíl: *Konceptuální návrh a ověření systému detekce anomálií z pohledu kybernetické bezpečnosti, založeného na strojovém učení v průmyslových řídících systémech*". Tento cíl je doplněn několika dílčími cíli. Tato **definice cílů je srozumitelná a správně zvolená**. Cíle stanovené v práci jsou autorem řešeny a plněny, nicméně jejich použitelnost musí být ještě ověřena konfrontací a kritickou diskusí s implementátory v praxi (např. odolnost průmyslových systémů, automotive, pracoviště řešící robustnost systémů vůči hrozbám Průyslu 4.0 a jejich řízená odolnost). Právě porovnání a diskuse s praxí na úrovni komerčních řešení je v tomto případě kriteriem úspěšnosti a progresu aplikovaného výzkumu.

Metody použité při vypracování disertační práce

Metody popsané výčtem na str .32 jsou použity v různých kombinacích a vytvářejí *vlastní vědeckou metodu* autora vyniklou teprve po seznámení se s celou prací. Bohužel, metoda, metodika a metodologie výzkumné vědecké práce demonstrující pokročilé schopnosti autora právě po stránce pokročilé vědecké práce, zde **nejsou popsány** a srozumitelně zachyceny, obzvláště metodologie vědecké práce není zcela srozumitelná a je intuitivní (byl autor práce účastníkem nějakého kurzu vědecké práce?).

Postup řešení problému a výsledky disertační práce, přínos doktoranda

Práce je rozdělena do 15 částí, z nichž prvních 8 kapitol (Úvod, Zhodnocení současného stavu, Cíle disertační práce, Zvolené metody zpracování, Teoretický rámec, Hlavní výsledky disertační práce, Přínos pro vědu a praxi, Závěr) je **přímo spojeno s řešením práce** a dalších 7 částí jsou seznamy (literatury, obrázků, tabulek, zkratek), přílohy, publikační aktivity a životopis autora.

Práce je psána velmi rozsáhle, mnohdy učebnicovým – výkladovým stylem, s přemírou používání zkratek a spojeními s ne vždy primárními informačními zdroji. Stejně tak např.

použití termínů na jedné straně z algebraické teorie čísel nebo parciálních derivací bez dostatečně hluboké souvislosti budí dojem **roztříštěnosti** a ne vždy pochopení významu základních termínů právě např. těchto matematických „nástrojů a objektů" – žádám o vyjádření a zdůvodnění.

Přístup autora k řešení problému a jeho postup odpovídá kombinaci více zvolených metod, kdy výsledky pak jsou spíše výzkumného, než aplikačního charakteru. Hlavní přínos práce doktoranda vnímám v tom, že **pojmenoval daný problém a pokusil se jej řešit výzkumnou metodou.** Výsledky práce jsou shrnuty v kapitole Závěr, ve které je potvrzena aplikační možnost navrženého a řešeného tématu. Problémem této práce je rozsáhlé používání řady matematických výrazů a vztahů, které jsou převzaty a brány jako vzorce bez zdůvodnění toho, jak vznikly, jak byly odvozeny. Uvítal bych alespoň v některých případech důsledné odvození, důvěra interpretačního charakteru spíše odráží **inženýrský** způsob-přístup k řešení.

Význam pro praxi a pro rozvoj vědního oboru

Význam práce pro praxi a rozvoj vědního oboru je v návrhu systému detekce – tedy v pokusu o jistý **systémový pohled na předmětnou oblast s využitím umělé inteligence**. Význam pro praxi by bylo třeba velmi přísně s reálnou praxí diskutovat a konfrontovat. Přijetí praxí je základním kritériem kvality aplikovaného výzkumu, která v reálném prostředí klade tyto otázky: je skutečně pro požadovaný technologický transfer úplný a tedy aplikovatelný?; byl návrh důkladně otestován a ověřen a diskutován? Tyto otázky nebyly v práci dostatečně hluboce odpovězeny.

Formální úprava disertační práce

Práce je psána českým jazykem, kapitoly na sebe navazují, text je prostý podstatných chyb a formálně splňuje nároky na doktorskou disertační práci v uvedeném oboru.

Dotazy k obhajobě

1) Dle použité literatury mnohokráte čerpáte ze zdrojů, které nejsou primárními. Jakým způsobem jste validoval jejich pravdivost?
2) Jaká je vazba mezi „ICS" a kritickou infrastrukturou státu (ke které se vyjadřujete např. na str. 125), jaká je relevance k tématu práce?
3) Vystavil jste svůj návrh reálným útokům?
4) Předpokládáte vy osobně další výzkumné pokračování v oblasti „ICS"?

Závěrečné vyjádření

Práci doporučuji k obhajobě před příslušnou komisí a v případě úspěšné obhajoby udělit titul Ph.D. v uvedeném oboru.

Ve Zlíně dne: 20.11.2020

prof. Mgr. Roman Jašek, Ph.D.

Kontaktní informace:
Ústav informatiky a umělé inteligence, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně
Nad Stráněmi 4511, 760 05 Zlín

OPONENTNÍ POSUDEK DISERTAČNÍ PRÁCE

Téma disertační práce:	Návrh a ověření systému detekce anomálií založeného na strojovém učení v průmyslových řídicích systémech
Studijní program/obor:	Inženýrská informatika
Autor práce:	Ing. Jan Vávra
Školitel:	doc. Ing. Luděk Lukáš, CSc.
Konzultant:	doc. Ing. Martin Hromada, Ph.D.
Oponent:	doc. Ing. Petr Hrůza, Ph.D.

Aktuálnost tématu disertační práce

Předložená disertační práce se zabývá problematikou kybernetické bezpečnosti v řídicích průmyslových systémech, které jsou využívány v kritické infrastruktuře. Právě systémy kritické infrastruktury jsou značně zatíženy novými hrozbami, mezi které řadíme také kybernetické útoky. Autor se konkrétně zaměřil na detekci anomálií založených na metodách strojového učení v průmyslových řídicích systémech. Z těchto důvodů hodnotím nejen téma, ale především rozsáhlost a systematické zpracování disertační práce jako **vysoce aktuální a přínosné** s potenciálem přispět k navržení nových bezpečnostních metodik, norem či standardů.

Splnění stanovených cílů v disertační práci

Cílem disertační práce bylo vytvořit systém detekce anomálií, který je založený na metodách strojového učení v oblasti kybernetické bezpečnosti u průmyslových řídicích systémů. K naplnění tohoto cíle si autor zvolil následující dílčí cíle:

- vymezení postupu identifikace kybernetických útoků pro průmyslové řídicí systémy,
- výběr, úprava a analýza vybraných datových setů průmyslových řídicích systémů a jejich parametrů, které budou využity pro detekci anomálií,
- identifikace a analýza algoritmů strojového učení vhodných pro oblast detekce anomálií,
- využití optimalizačních technik pro zvýšení detekčních schopností zvoleného řešení,
- zhodnocení možnosti interpretace detekovaných anomálií,
- vytvoření algoritmu pro detekci anomálií, založeném na strojovém učení,
- ověřování, testování a hodnocení navrženého řešení.

Výzkumné cíle jsou velmi rozsáhlé a systematicky pokrývají celý rozsah dané problematiky (od výběru dat, jejich atributů, provedení analýzy nad těmito daty, až po ověření systému detekce anomálií a jejich implementace pomocí algoritmů strojového učení). Velice oceňuji způsob, jakým autor disertační práce přistoupil k řešení daného problému. Neboť tento způsob vyžadoval provedení velkého množství zkoumání, analýz a experimentů. **V kontextu těchto skutečností shledávám cíl, jakož i dílčí cíle splněné v plném rozsahu.** Předložená disertační práce má vysokou úroveň nových poznatků.

Metody použité při vypracování disertační práce

V disertační práci bylo použito větší množství výzkumných metod, což je dáno povahou a rozsáhlostí řešené problematiky (metoda analýzy, metoda syntézy, metoda modelování, metoda komparace, metoda experimentu, metody matematické statistiky, metoda indukce).
Metodu modelování použil pro vytvoření prediktivního modelu pro klasifikaci zvoleného datového setu. Pro analýzu zkoumání těchto datových setů a pro oblast vývoje vhodných postupů při identifikaci anomálií v rámci dizertační práce využil metodu matematické statistiky. Metodu experimentu následně aplikoval k ověření předpokladů v oblasti detekce anomálií. Použití všech výše uvedených výzkumných metod shledávám jako adekvátní a vhodné pro bádání v dané oblasti. **Celkově mohu konstatovat, že použité metody jak svým rozsahem, tak i jejich vhodným použitím v disertační práci dávají výsledkům vysokou relevanci.**

Postup řešení problému, výsledky disertační práce a konkrétní přínos práce doktoranda

Popsaný postup řešení daného problému je v disertační práci unikátní hned z několika důvodů, z nichž nejdůležitější jsou rozsah a kvalita provedených experimentů z oblasti strojového učení a následná validace navrženého postupu ve formě vytvořeného systému pro detekci anomálií. Z výše uvedeného je patrné, že autor ve své disertační práci provedl značné množství experimentů. Systém pro detekci anomálií autor rozdělil do čtyř částí. V první mapoval kybernetické hrozby pro řídicí průmyslové systémy pomocí nástrojů pro dolování databází a nástroje Shodan. Ve druhé se zaměřil na výzkum spojený s datovou úpravou vstupních dat, nad kterými provedl všechny experimenty. Ve třetí části využil algoritmů strojového učení pro stanovení postupu detekce anomálií s následnou optimalizací algoritmů. V této části práce navrhl nový postup pro detekci anomálií pomocí multikriteriálního hodnocení pro řešení vícekriteriální optimalizace. Autor v práci porovnává jednotlivé optimalizační algoritmy. Provedl rozsáhlý výzkum pomocí experimentů se zaměřením na optimalizaci algoritmů strojového učení prostřednictvím pěti metrik. Ve čtvrté pak následně získané výsledky interpretoval do systému pro detekci anomálií za využití reverzních postupů. Proces interpretace autor popsal na dvou případech. V prvním případě byla interpretace založena na neuronové síti využívající postup pro detekci anomálií a ve druhém případě byl využit algoritmus strojového učení RF. Zde využil paralelní nasazení algoritmu IF pro účel interpretace anomálií. Dále pomocí interpretace našel příčiny falešných poplachů, které mu napomohly upravit klasifikační model pro potřeby detekce anomálií.

Význam pro praxi a pro rozvoj vědního oboru

Význam práce pro rozvoj vědního oboru a praxi je v oblasti **systémového přístupu** k řešení tématu práce.
Výsledky publikované v předložené disertační práci jsou přínosné zejména pro:

- odborníky z řad akademické obce,
- experty a společnosti zabývající se informační bezpečností, zejména pak bezpečností průmyslových řídicích systémů.

Pro odborníky z řad akademické obce bude nejzajímavější problematika tvorby pro detekci anomálií v řídicích průmyslových systémech, které lze nasadit na reálný systém. Přínosné jsou také experimenty, které jsou především zaměřeny na optimalizaci algoritmů strojového učení prostřednictvím pěti metrik.

Pro bezpečnostní experty a společnosti zabývající se informační bezpečností, zejména pak bezpečností v řídicích průmyslových systémech, kde autor představil systém umožňující detekci neznámých kybernetických útoků a navrhl dvě potenciální řešení pro ochranu těchto systémů.

Rovněž oceňuji skutečnosti, že obsah práce není pouze teoretický, ale přináší celou řadu konkrétních postupů či vylepšení.

Formální úprava a jazyková úroveň disertační práce

Práce je psána v českém jazyce, který má spisovnou formu a zároveň splňuje nároky kladené na vědecké publikace. Navzdory skutečnosti, že je práce rozsáhlá, její členění je přehledné a struktura má celistvý charakter. Řazení jednotlivých kapitol je koncepční, kdy poznatky předchozí kapitoly podporují kapitolu následující. Celkově lze říci, že předložený text splňuje všechny formální a jazykové nároky kladené na doktorskou disertační práci.

Publikační a další vědecko výzkumná činnost doktoranda

Předložená publikační činnost autora odpovídá požadavkům kladených na studenty doktorských studijních programů. Autor publikoval své výsledky několika mezinárodních a národních konferencí, většinou společně s konzultantem docentem Hromadou.

Dotazy k obhajobě

Závěrem mohu konstatovat, že předložená disertační práce splňuje po faktické i formální stránce požadavky kladené na disertační práci, obsahuje nové, zajímavé a prakticky využitelné výsledky, které autor publikoval.

Při obhajobě disertační práce požaduji reakci studenta na následující problémy:

1. Proč jste při transformaci dat použil algoritmus PCA?

2. Při experimentu jste použil 5 hodnotících metrik. Která z nich byla pro vás při experimentech nejdůležitější a proč?

3. Pro detekci anomálií jste použil čtyři algoritmy strojového učení a tří datových setů. Algoritmus OCSVM jste vyloučil na základě špatných výsledků. Který z těch zbývajících tří byl pro provádění experimentů nejvíce vhodný a proč?

Závěrečné vyjádření

Ve smyslu ustanovení § 47 zákona č. 111/1998 Sb. o vysokých školách doporučuji disertační práci Ing. Jana Vávru k obhajobě před příslušnou komisí a na základě úspěšné obhajoby navrhuji udělit titul philosophiae doctor (Ph.D.) v doktorském studijním programu Inženýrská informatika.

V Brně dne 29. listopadu 2020 .....

ŽILINSKÁ UNIVERZITAV ŽILINE
Fakulta riadenia a informatiky
Katedra informačných sietí

Doc. Mgr. Ondrej Šuch, PhD.
Katedra informačných sietí FRI
Žilinská univerzita v Žiline
Tel.: (41) 513 4327
e-mail: ondrej.such@fri.uniza.sk

POSUDOK DOKTORANDSKEJ DIZERTAČNEJ PRÁCE

Autor práce: Ing. Ján Vávra

Názov témy: Návrh a ověření systému detekce anomálií založeného na strojovém učení v průmyslových řídicích systémech

Téma práce je vysoko aktuálna, nakoľko bezpečnosť IoT zariadení je často prehliadaná medzera v zabezpečení IT infraštruktúry organizácií. Narušenie činnosti priemyselných zariadení v Industry 4.0 môže mať katastrofálne dôsledky, čo autor správne postrehol. Takisto správne poznamenáva, že riešenie problémov v zabezpečení priemyselných IoT zariadení je ťažšie oproti osobným počítačom alebo serverom.

Autor si stanovil za cieľ "*Konceptuální návrh a ověření systému detekce anomálií z pohledu kybernetické bezpečnosti, založeného na strojovém učení, v průmyslových řídicích systémech*". Tento cieľ vyžadoval vykonanie ôsmych čiastkových krokov, ako je uvedené na strane 34 práce. Tieto boli v práci úspešne vykonané, snáď s výnimkou posledného a to *Interpretace výsledků*. Ocenil by som podrobnejšie vysvetlenie stavu riešenia tohto kroku počas obhajoby, napr. podrobnejším vysvetlením diagramu 46. Keďže však interpretáciu vnímam ako nadstavbovú a netriviálnu métu, ktorá ostáva otvoreným výskumným problém, cieľ práce samotnej považujem za splnený.

Autor postupoval pri vypracovaní riešenia systematicky. Logicky zdôvodnil použitie state-of-the-art metód, krátko ich vysvetlil a dobre zdokumentoval svoje riešenie. Rozsiahle experimenty sú zhodnotené v prílohách na stranách 158-268. Použité štatistické metódy boli vhodne zvolené a poskytujú objektívny pohľad na kvalitu navrhovaného riešenia. Množstvo prezentovaných experimentov je vysoko nad rámec štandardnej doktorandskej práce a oceňujem motiváciu doktoranda tieto experimenty vykonať a vyhodnotiť. Množstvo citovanej literatúry je primerané. Do pozornosti autora by som však dal ďalšie dve práce v odbore. Prvá z nich ilustruje ťažkosti s detekciou anomálií už v dvoch dimenziách [1], čo korešponduje so správnym upozornením autora na problém prekliatia dimenziou (str. 37 práce). Druhá poskytuje referenčnú úlohu s reálnymi dátami pre vyhodnocovanie algoritmov na detekciu anomálii [2].

Autorova práca má priamu využiteľnosť pre tvorbu zabezpečovacích systémov v priemyselnej praxi. Osobne by som vyzdvihol dovedenie výskumu detekcie anomálií do plne funkčnej demonštrácie systému, ktorý je schopný detegovať anomálie prevádzky, no popritom má nízke množstvo falošných poplachov. Veľmi cenným pre vedeckú prax je zistenie, že metóda one class SVM, ktorá je veľmi často využívaná na detekciu anomálií, sa ukázala oveľa menej efektívnou oproti novším metódam. Takisto hodnotné je aj preukázanie užitočnosti optimalizovania hyperparametrov evolučným algoritmom, ktoré výrazne pomohlo znížiť kritickú metriku M_{FPR}pre isolation forest.

Formálna stránka práce je adekvátna, no mohla by byť ešte lepšia s dôslednejším využitím moderných typografických nástrojov (LaTeX, Word, alebo Markdown), čo by umožnilo autorovi vyhnúť sa ako lexikálnym chybám, tak aj problému nesprávnych referencií.

Publikačnú činnosť autora hodnotím ako veľmi dobrú. Tri zahraničné pracovné stáže uskutočnené počas doktorandského štúdia majú prísľub ešte viac podporiť budúcu tvorivú činnosť autora práce.

ŽILINSKÁ UNIVERZITAV ŽILINE
Fakulta riadenia a informatiky
Katedra informačných sietí

Na záver odporúčam uvedenú prácu k obhajobe apo jej úspešnom obhájení navrhujem Ing. Janovi Vávrovi

udeliť vedecko-akademickú hodnosť philosophiae doctor (PhD.) v študijnom obore Inženýrska informatika

Žilina, 29.11.2020

doc. Mgr. Ondrej Šuch, PhD.

Referencie

[1] M. J. R. Healy, Rao's Paradox Concerning Multivariate Tests of Significance, Biometrics, Vol. 25, No. 2 (Jun., 1969), pp. 411-413

[2] S. Ahmad et al, Unsupervised real-time anomaly detection for streaming data, Neurocomputing, Vol. 262, No. 1, (Nov., 2017), pp. 134-147.