RADA NAUKOWA DYSCYPLINY
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

zaprasza na

OBRONĘ ROZPRAWY DOKTORSKIEJ

mgr. inż. Wojciecha Tadeusza Niewolskiego

która odbędzie się w dniu **13 listopada 2023 roku,** o godzinie **16:00** w trybie stacjonarnym

Temat rozprawy:

„System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych”

Promotor: prof. dr hab. inż. Zbigniew Kotulski – Politechnika Warszawska

Recenzenci: dr hab. inż. Piotr Chołda, prof. uczelni – Akademia Górniczo-Hutnicza im. Stanisława Staszica

dr hab. inż. Jacek Rak, prof. uczelni – Politechnika Gdańska

dr hab. inż. Grzegorz Kołaczek, prof. uczelni – Politechnika Wrocławska

Obrona odbędzie się w Sali 478 Gmachu Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, adres: ul. Nowowiejska 15/19, 00-665 Warszawa.

Z rozprawą doktorską i recenzjami można zapoznać się w Czytelni Biblioteki Głównej Politechniki Warszawskiej, Warszawa, Plac Politechniki 1.

Streszczenie rozprawy doktorskiej i recenzje są zamieszczone na stronie internetowej: https://www.bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-po-30-kwietnia-2019-r/Rada-Naukowa-Dyscypliny-Informatyka-Techniczna-i-Telekomunikacja/mgr-inz.-Wojciech-Tadeusz-Niewolski

Przewodniczący Rady Naukowej Dyscypliny
Informatyka Techniczna i Telekomunikacja
Politechniki Warszawskiej
dr hab. inż. Jarosław Arabas, prof. uczelni

Warszawa, 24.04.2023

Wojciech Niewolski
(imię i nazwisko)

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

„System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych"

W rozprawie przedstawiono ideę i projekt adaptacyjnego systemu bezpieczeństwa przeznaczony dla usług realizowanych w nowych architekturach sieciowych. Opracowany w ramach pracy system AraMIS (Adapted 5G+ MultiCloud Intelligent Security) umożliwia dopasowanie poziomu bezpieczeństwa, zależnie od typu zagrożenia, charakterystyki serwisu, jak i polityki ochrony zdefiniowanej przez właściciela aplikacji. Wspomniana cecha stanowi jeden z głównych wyróżników spośród wielu obecnych rozwiązań, których przeglądu dokonano przed przystąpieniem do realizacji systemu AraMIS. Analiza prac naukowych oraz rozwiązań komercyjnych potwierdziła, że temat zautomatyzowanego systemu adaptacji bezpieczeństwa nie był jak dotąd rozważany.

W celu potwierdzenia zasadności tworzenia systemu AraMIS, w pracy przedstawiono odmienne potrzeby wobec poziomu bezpieczeństwa, jakie muszą być spełnione w różnych sektorach rynku ICT (Information and Communication Technologies). W tym celu opisano możliwe scenariusze realizacji usług rozproszonych, wraz ze schematami ich integracji z sieciami mobilnymi. Dla wymienionych architektur dokonano przeglądu zagrożeń oraz stosowanych obecnie metod do klasyfikacji i oceny ich ryzyka, zgodnie z obowiązującymi standardami. Analiza opisanych powyżej serwisów, wykazała potrzebę zastosowania adaptacyjnego bezpieczeństwa, który nie jest oferowany przez istniejące systemy ochrony.

Następnie w pracy przedstawiono architekturę systemu AraMIS uwzględniającą opis każdego z używanych przez niego elementów. W pracy ujęto wyniki skuteczności detekcji i klasyfikacji komponentów systemu AraMIS, wraz z analizą porównawczą innych metod i algorytmów ochrony bezpieczeństwa. Zawarto także wnioski z procesu optymalizacji metod detekcji, zarówno pod kątem skuteczności jak i optymalizacji zużycia zasobów, które potwierdziły poprawność opracowanych metod i dowiodły słuszności tez pracy.

Dodatkowo w pracy przedstawiono metody do usprawnienia procesu orkiestracji w środowiskach brzegowych, w szczególności związane z realizacją procesu bezpieczeństwa. Zaprezentowano analizę możliwości istniejących interpreterów polityki bezpieczeństwa, w porównaniu do autorskiej propozycji zapisu polityki, za pomocą grafów logicznych i oprogramowania NodeRED. Wspomniany komponent został wdrożony w firmie Orange. W pracy zawarto także opis opracowanego rozwiązania MEC Enabler, które służy do zwiększenia ochrony w warstwie sieci oraz metodę jego integracji z systemem AraMIS.

Słowa kluczowe: adaptacyjne bezpieczeństwo, system zautomatyzowanej ochrony, detekcja, klasyfikacja, 5G MEC

Wojciech Niewolski
(podpis doktoranta)

Wrocław 18.08.2023r.

Dr hab. inż. Grzegorz Kołaczek, prof. uczelni
Katedra Informatyk i Inżynierii Systemów
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska
ul. Wybrzeże Wyspiańskiego 27
50-370 Wrocław

Recenzja rozprawy doktorskiej

Autor:

mgr inż. Wojciech Niewolski

Tytuł:

„System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych"

Promotor:

Prof. dr hab. Zbigniew Kotulski,
Politechnika Warszawska

Niniejsza opinia została przygotowana na prośbę dr hab. inż. Jarosława Arabasa, prof. uczelni, Przewodniczącego Rady Dyscypliny Informatyka Techniczna i Telekomunikacja z dnia 20.06.2023r.

1. Problem badawczy i jego znaczenie

Recenzowana rozprawa jest związana z problematyką zapewnienia bezpieczeństwa złożonym, dynamicznym systemom informatycznym. W szczególności rezultaty rozprawy dotyczą zagadnień zautomatyzowanego, adaptacyjnego zapewniania bezpieczeństwa usług. Autor rozprawy skupia się na możliwości dostosowania metody ochrony do typu zagrożenia i charakterystyki serwisu z jednoczesnym uwzględnieniem polityki ochrony zdefiniowanej przez właściciela aplikacji.

Analiza literatury przedmiotu oraz aktualnych przedsięwzięć o charakterze wdrożeniowym potwierdza istotność wybranej przez autora rozprawy problematyki badawczej. W szczególności wzrost złożoności systemów, ich heterogeniczność oraz dynamika rozwoju, z drugiej zaś strony różnorodność wymagań definiowanych przez użytkowników, przy jednoczesnym wzroście zarówno liczby zagrożeń, jak i też oczekiwań dotyczących bezpieczeństwa usług informatycznych sprawia, że uzyskane w ramach przedłożonej rozprawy rezultaty mają znaczący wpływ na rozwój badań w obszarze bezpieczeństwa w dyscyplinie naukowej informatyka techniczna i telekomunikacja.

2. Kompozycja rozprawy

Recenzowana rozprawa liczy 260 stron. Została ona podzielona na siedem rozdziałów oraz zawiera trzy załączniki. W pracy zamieszczono również spis rysunków, spis tabel i skrótów oraz bibliografię złożoną z 276 pozycji literaturowych.

Układ i zawartość rozdziałów merytorycznych jest zasadniczo poprawna. W pierwszym rozdziale w sposób syntetyczny przedstawiony jest cel badań oraz sformułowana jest główna teza badawcza rozprawy. Ponadto wymienione są główne rezultaty naukowe rozprawy oraz scharakteryzowana została struktura dalszej części rozprawy.

Drugi rozdział zawiera wprowadzenie do zagadnień związanych z usługami chmurowymi w kontekście sieci nowej generacji w tym sieci 5G. W pierwszej części rozdziału omówione są różne modele i architektury świadczenia usług chmurowych. Następnie przedstawione są możliwości realizacji dostępu mobilnego do środowisk chmurowych, a w kolejnej części rozdziału zaprezentowane są koncepcje integracji systemu 5G i MEC (Multi-access Edge Computing) oraz scharakteryzowane są nowe potrzeby i trendy usług wertykalnych.

Kolejny rozdział dotyczy zagrożeń i ochrony usług w środowisku MEC. W tym rozdziale omówione są zagadnienia związane z oceną zagrożeń i zarządzaniem ryzykiem, metodami zapobiegania zagrożeniom w środowisku MEC oraz dokonano przeglądu literatury w zakresie systemów do automatycznej ochrony.

Rozdział czwarty przedstawia projekt systemu adaptacji bezpieczeństwa, na który składa się analiza istniejących metod monitorowania aplikacji chmurowych oraz opis proponowanej architektury systemu monitoringu. W tym rozdziale również przedstawiona jest dyskusja nad możliwością ograniczenia zapotrzebowania na energię elektryczną detektora zdarzeń bezpieczeństwa oraz przedstawiono architekturę i sposób implementacji interfejsu sterowania dla zaproponowanego systemu bezpieczeństwa.

Kolejny rozdział zawiera wyniki przeprowadzonych badań nad skutecznością detekcji i klasyfikacji incydentów dla projektowanego systemu wraz z charakterystyką działań prowadzących do optymalizacji jego działania.

Rozdział szósty koncentruje się nad efektywnością procesu orkiestracji w środowiskach przetwarzania Edge Computing. Również w tym rozdziale zawarto rozważania dotyczące problemów w implementacji polityki bezpieczeństwa w systemach informatycznych.

Końcowy rozdział zawiera syntetyczne podsumowania otrzymanych rezultatów oraz charakterystykę możliwych prac związanych z dalszym rozwojem zaproponowanego w rozprawie rozwiązania.

3. Oryginalne osiągnięcia

Do szczególnych oryginalnych elementów rozprawy należy zaliczyć:

- zaprojektowanie architektury referencyjnej Multi Access Edge Computing (MEC) dającej możliwość integracji z różnorodnymi metodami dostępu oraz dokonanie przykładowej implementacji i testów rozwiązania w zgodzie z zaproponowanymi wytycznymi projektowymi
- opracowanie interoperacyjnego i przenaszalnego systemu monitorowania na potrzeby gromadzenia danych charakteryzujących aktualny poziom bezpieczeństwa aplikacji
- opracowanie metody detekcji anomalii z uwzględnieniem wymagań dotyczących ograniczenia zapotrzebowania na konsumpcję energii elektrycznej
- opracowanie i implementację dynamicznego modelu polityki bezpieczeństwa wraz z interpretatorem umożliwiającym konfigurowalny i zautomatyzowany proces detekcji oraz reakcji, uwzględniający dane kontekstowe
- zaprojektowanie i implementację metody ochrony dostępu, dla aplikacji uruchamianych w MEC (MEC Enabler) wraz funkcją umożliwiającą anonimizację wybranych połączeń
- implementację demonstratora systemu AraMIS umożliwiającego dopasowanie poziomu bezpieczeństwa, zależnie od typu zagrożenia, charakterystyki serwisu, jak i polityki ochrony zdefiniowanej przez właściciela aplikacji

Dorobek publikacyjny autora wskazany jako związany z przedłożoną rozprawą składa się z dziewięciu publikacji, w tym w IEEE Access (IF=3,9 oraz 100 pkt. na liście MEiN). Dorobek publikacyjny świadczy o tym, iż przedstawione w rozprawie wyniki prac badawczych zostały również pozytywnie zweryfikowane podczas procesu recenzyjnego oraz także poddane dyskusji w trakcie wystąpień na konferencjach.

Powyższe osiągnięcia należy uznać za oryginalne i znaczące dla dyscypliny naukowej informatyka techniczna i telekomunikacja. Na tej podstawie Recenzent opiera swoją ogólną pozytywną ocenę rozprawy. Osiągnięcia te stanowią równocześnie potwierdzenie postawionej przez Autora głównej tezy pracy, czyli pokazują, iż możliwe jest zbudowanie systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych.

4. Uwagi krytyczne

Przedłożona do recenzji rozprawa jest pod względem merytorycznym i redakcyjnym w przeważającej części napisana poprawnie. W ocenie Recenzenta Autor nie ustrzegł się jednak również pewnych błędów, niedociągnięć i nieścisłości. Poniżej zostały zamieszczone najważniejsze uwagi krytyczne do treści, jak i formy pracy.

a. Uwagi natury ogólnej

1. Analiza literatury. W rozprawie analiza literatury pojawia się w kilku miejscach. W opinii recenzenta korzystniejsze dla rozprawy i dla jej czytelności byłoby dokonanie takiej analizy w jednym miejscu i w sposób metodyczny (np. przy zastosowaniu metody systematycznego przeglądu literatury). Dałoby to możliwość bardziej precyzyjnego i spójnego przedstawienia prezentowanego problemu na tle aktualnych osiągnięć naukowych.
2. Granularność modułów. Autor rozprawy rozpatruje oddzielnie moduł wykrywania anomalii i moduł klasyfikacji zdarzeń. W opinii recenzenta zasadne byłoby rozważenie możliwości integracji tych dwóch modułów w jeden, w celu zapewnienia większej wydajności i efektywności systemu zarządzania bezpieczeństwem.
    i. Czy możliwość klasyfikacji zdarzenie jako np. atak typu „brute force" nie jest wystarczającą informacją dla całego systemu zarządzania bezpieczeństwem, np. umożliwiającą podjęcie skutecznej reakcji?
    ii. Czy istnieją anomalie, które nie będą sklasyfikowane na późniejszym etapie i jaki to może mieć wpływ na działanie systemu zarządzania bezpieczeństwem?
    iii. Jak rozdzielenie tych funkcji wpływa np. na ograniczenie zapotrzebowania na energię.
3. Narzędzia w implementacji. W przedstawionej implementacji opracowanej architektury systemu zarządzania bezpieczeństwem wykorzystano wybrane narzędzia (np. OpenVSwitch, Suricata, itd.). W opinii recenzenta wybór ten jest arbitralny. Warto byłoby rozważyć opracowanie metody wyboru narzędzi, np. w oparciu o bardziej ogólne ale również konkretne wymagania dotyczące np. możliwości eksportu informacji dotyczącej monitorowanego obiektu w formacie json, możliwości generowania zdarzeń z zadanym odstępem czasu, itp.
    i. Czy dokonany wybór ma/może mieć wpływ na interoperacyjność, przenaszalność i efektywność zaimplementowanego rozwiązania?.
4. Wektor danych. Wykorzystywane w pracy algorytmy uczenia maszynowego korzystają ze zbioru danych określonego na 240/100 wyselekcjonowanych cech opisujących system. Jaki był oryginalny rozmiar wektora cech? Dlaczego zdecydowano się na wykorzystanie takiego szerokiego wektora cech skoro w świetle wyników z rozdziału 4 znaczna ich liczba nie jest znacząca informacyjnie? Czy oprócz

przedstawionej w rozprawie metody selekcji cech autor rozważał możliwości wykorzystania metod ekstrakcji cech? Czy były prowadzone analizy reprezentatywności analizowanego zbioru danych dla tak szerokiego wektora cech?

5. Diagramy. Jednym z istotnych elementów pracy jest projekt złożonego systemu. Czy w trakcie projektu były wykorzystywane metody modelowania np. z wykorzystaniem diagramów UML, BPMN, lub innych?
6. Anomalie. W rozdziale 5 przedstawiono test skuteczności działania algorytmów detekcji i klasyfikacji. W tym celu zasymulowane zostały wybrane scenariusze ataków, przy czym proporcja stanu normalnego do anomalnego (ataku) wyniosła 144/60. Jak taka proporcja ma się do potencjalnie możliwych do wystąpienia sytuacji w środowisku rzeczywistym i jaki to może mieć wpływ na poprawną interpretację wyników eksperymentu?
7. Precyzja języka.
    i. Autor rozprawy posługuje się wieloma terminami bez określenia precyzyjnego i właściwego dla nich kontekstu (np. optymalizacja), bądź stosuje zamiennie terminy o różnym znaczeniu (np. funkcja i funkcjonalność, adaptacja do polityki bezpieczeństwa oraz adaptacja bezpieczeństwa i adaptacja komponentów bezpieczeństwa, metody i mechanizmy oraz systemy), lub w przekonaniu recenzenta, w nie do końca właściwej formie (np. przenośny vs przenaszalny, adaptacja danych wejściowych). Również nie udało się ustrzec Autorowi pewnych niezręczności językowych (np. „ocena parametrów przy pomocy twierdzenia Shannon”). Niektóre z powyższych błędów mogą niekorzystnie wpływać na czytelność i możliwość poprawnej interpretacji treści rozprawy.
    ii. W pracy zabrakło jasnego zdefiniowania kluczowych dla rozprawy terminów takich jak adaptacja poziomu bezpieczeństwa, dynamiczna adaptacja, wydajność, skuteczność, automatyzacja (np. w taki sposób jak to zostało zrobione w pkt. 5.4)
8. Dostępność kodu źródłowego. Obecnie powszechnie stosowaną praktyką jest udostępnianie kodu, zwłaszcza kodu związanego z realizowaną pracą badawczą. Autor mógł udostępnić wytworzony kod, np. w postaci ogólnodostępnego repozytorium. Stanowić mogłoby to dodatkową cenną możliwość upowszechnienia i rozwoju przeprowadzonych prac badawczych.

b. Uwagi natury szczegółowej

1. Rysunki i tabele w rozdziale 2 posiadają niewłaściwą numerację.
2. Sposób prezentacji elementów graficznych w wielu miejscach wersji drukowanej rozprawy jest nieczytelny, a przez to również ogranicza możliwość analizy i interpretacji.

3. Niektóre dane prezentowane w rozprawie pozostawione bez szerszego komentarza mogą mieć charakter kontrowersyjny/dyskusyjny (np. dane w Tabeli 1.3 – mały wpływ ataków typu „data breach” w sektorze „healthcare”).
4. Nie jest jasne dla Recenzenta jak należy interpretować dane w kolumnie „Okres aktywności” w Tabeli 4.9. i co jest podstawą do takich, a nie innych wartości występujących w tej kolumnie.
5. Autor nie ustrzegł się błędów językowych i interpunkcyjnych.

5. Konkluzja

Zgodnie z zapisami ustawy „Prawo o szkolnictwie wyższym i nauce” (art. 187.1) z dnia 20 lipca 2018 r. ocenie podlega, czy rozprawa doktorska prezentuje ogólną wiedzę teoretyczną kandydata w dyscyplinie, umiejętność samodzielnego prowadzenia pracy naukowej oraz czy rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej.

Doktorant wykazał się w recenzowanej rozprawie obszerną wiedzą z zakresu poruszanej tematyki bezpieczeństwa systemów informatycznych i telekomunikacyjnych. Autor rozprawy w wyniku studiów literaturowych poprawnie zidentyfikował istotne problemy badawcze, a na tej podstawie sformułował tezę pracy oraz opracował scenariusze badawcze i przedstawił, w jaki sposób zostały one przeprowadzone w ramach podjętych prac. Pozwala to na stwierdzenie faktu spełnienia wymogów ustawy przez mgr. inż. Wojciecha Niewolskiego w dyscyplinie Informatyka Techniczna i Telekomunikacja.

Recenzowana rozprawa przedstawia ponadto oryginalne rozwiązanie problemu z zakresu adaptacyjnych metod gwarantowania wymaganego poziomu bezpieczeństwa systemom i usługom informatycznym. Ponadto autor rozprawy przedstawił sposób zastosowania wyników przeprowadzonych badań naukowych w sektorze telekomunikacyjnym gospodarki, a przez to przedłożona rozprawa również wypełnia wymagania ustawy w zakresie umiejętności prowadzenia samodzielnej pracy naukowej.

Biorąc powyższe pod uwagę stwierdzam, że praca mgr. inż. Wojciecha Niewolskiego pt. „System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych” spełnia wszystkie wymagania stawiane rozprawom doktorskim w świetle stosownej ustawy. Wnoszę o jej przyjęcie i dopuszczenie do jej publicznej obrony.

Grzegorz Kołaczek

POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Gdańsk, 14.08.2023 r.

Dr hab. inż. Jacek Rak, prof. PG
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Recenzja rozprawy doktorskiej

Tytuł: System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych

Autor: Mgr inż. Wojciech Niewolski

Rozprawa doktorska mgra inż. Wojciecha Niewolskiego dotyczy problemu budowy systemu bezpieczeństwa, którego właściwości i zasady funkcjonowania są dopasowane adekwatnie do potrzeb świadczonych usług oraz architektur sieciowych, w ramach których te usługi funkcjonują (postulat adaptacji). Rozpatrywany problem jest niewątpliwie ważny i aktualny z uwagi na szereg zmieniających się dynamicznie uwarunkowań dotyczących m.in. ewolucji klas usług, różnorodności charakterystyk architektur (wykorzystujących np. strategie Cloud Computing, Edge Computing, Multi Access Edge Computing), jak i postępujących dalszych zmian tychże architektur. Niemniej istotną w tym zakresie jest dynamika zmian charakterystyk samych ataków sprawiająca, że opracowane metody zaradcze w zakresie detekcji, klasyfikacji i przeciwdziałania atakom, z biegiem czasu tracą na znaczeniu. Niewątpliwie słuszny jest zatem kierunek badań niniejszej rozprawy dotyczący konstrukcji systemu adaptacji poziomu bezpieczeństwa do konkretnych (zmiennych w czasie) uwarunkowań.

Oceniana rozprawa doktorska ukazuje autorskie rezultaty w rozpatrywanym obszarze, w tym w szczególności w zakresie: (1) projektu systemu bezpieczeństwa oferującego dopasowanie poziomu bezpieczeństwa do charakterystyk zagrożenia, cech architektury sieci oraz wymagań wynikających z założonej polityki ochrony; (2) analizy skuteczności zrealizowanego systemu.

Rak

Oceniana rozprawa doktorska została napisana w języku polskim i składa się z siedmiu rozdziałów numerowanych oraz kilku części nienumerowanych, w tym wykazu literatury, skrótów, tabel, rysunków oraz trzech załączników. Jej struktura jest ogólnie poprawna i odpowiada zwyczajowym wymaganiom stawianym rozprawom doktorskim. Jednocześnie należy zaznaczyć, że oceniana rozprawa doktorska jest także wynikiem realizacji tzw. „doktoratu wdrożeniowego", a więc dotyczącego realnych badawczych problemów praktycznych (w tym przypadku związanych z działalnością firmy Orange).

1. Jaki jest problem naukowy, cel i teza rozprawy oraz czy zostały one trafnie i jasno sformułowane?

Problemem naukowym ocenianej rozprawy jest opracowanie mechanizmu dopasowania poziomu bezpieczeństwa adekwatnie do charakterystyk świadczonych usług sieciowych, właściwości architektury systemu oferującego te usługi, jak i przyjętej polityki bezpieczeństwa.

Sformułowaną w tym kontekście na stronie 8 tezę rozprawy mówiącą o ***możliwości zbudowania systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych*** należy uznać za postawioną jednoznacznie i właściwie, a trud jej wykazania jako adekwatny dla tez rozpraw doktorskich.

Celem pracy jest więc próba opracowania systemu bezpieczeństwa spełniającego powyższe wymagania, a więc którego właściwości mogłyby dowieść prawdziwości postawionej tezy.

Aby zrealizować postawiony cel badawczy i wykazać tezę rozprawy, Doktorant wykonał pięć głównych zadań badawczych dotyczących:

(1) projektu i implementacji referencyjnej architektury referencyjnej Multi Access Edge Computing,
(2) realizacji uniwersalnego systemu pozyskiwania danych w zakresie oceny poziomu bezpieczeństwa aplikacji,
(3) opracowania modelu detektora anomalii przy wykorzystaniu ML/VAE,
(4) realizacji dynamicznego modelu polityki bezpieczeństwa uwzględniającego dane kontekstowe,
(5) projektu i implementacji systemu ochrony dostępu dedykowanego aplikacjom uruchomionych w MEC, jak i anonimizacji części połączeń

oraz trzy zadania pomocnicze w zakresie:

(a) analizy danych przy wykorzystaniu technik AI/ML,
(b) konstrukcji systemu generowania oraz uruchamiania modeli detektorów i klasyfikatorów,
(c) analizy skuteczności i wydajności autorskich komponentów

ukazane na stronach 8 i 9 rozprawy.

Zakres tychże zadań nie budzi moich zastrzeżeń i jest moim zdaniem adekwatny w stosunku do postawionej tezy.

2. Na czym polega oryginalny dorobek Autora i jakie jest znaczenie poznawcze lub przydatność praktyczna dla nauki bądź techniki?

Do oryginalnego dorobku Autora niniejszej rozprawy doktorskiej można moim zdaniem zaliczyć następujące rezultaty:

1) dyskusję w zakresie właściwości modeli i architektur świadczenia usług chmurowych wraz z charakterystyką dominujących scenariuszy dostępu do usług rozproszonych, jak i charakterystyką możliwych schematów integracji tychże architektur z sieciami mobilnymi (w szczególności realizacja dostępu mobilnego do środowisk chmurowych oraz integracja systemu 5G i MEC) ukazane w rozdziale 2 rozprawy,

2) szczegółowy opis zagrożeń w obszarze bezpieczeństwa (w tym w szczególności ich kilkustronicowa szczegółowa klasyfikacja w tabeli 3.1) w kontekście architektur obecnie wykorzystywanych systemów wraz z klasyfikacją cyberataków ukazane w rozdziale 3,

3) rozszerzenie rozdziału 3 rozprawy o przedstawienie i analizę właściwości mechanizmów zarządzania ryzykiem incydentów cyberbezpieczeństwa wraz z opisem metod zapobiegania tymże zagrożeniom w środowisku MEC (tabela 3.4), jak i przegląd oraz analiza właściwości systemów automatycznej ochrony przed cyberatakami,

4) propozycję adaptacyjnego systemu bezpieczeństwa AraMIS szczegółowo opisaną w rozdziale 4. W szczególności na uwagę zasługuje zawarty w nim opis systemu przenośnego monitoringu, autorska propozycja modelu sieci neuronowej opracowanego przez Doktoranta w celu opracowania detektora anomalii, jak i szczegółowy opis implementacji interfejsu do sterowania systemem AraMIS,

5) analizę właściwości systemu AraMIS przedstawioną w rozdziale 5 rozprawy, w tym w szczególności szczegółowy opis scenariuszy testów, opis metod używanych do analizy wyników, oraz szczegółową analizę wyników uzyskanych w przygotowanym przez Doktoranta w tym celu środowisku eksperymentalnym dotyczących skuteczności proponowanego rozwiązania w zakresie detekcji oraz klasyfikacji cyberataków w zestawieniu z wynikami systemów referencyjnych. Wyniki te ukazały największą skuteczność dla detektorów zaprojektowanych przez Doktoranta na bazie modeli uczenia maszynowego na podstawie sieci neuronowej,

6) zawartą w rozdziale 6 rozprawy propozycję sposobów usprawnień mechanizmu orkiestracji w obszarach brzegowych systemu oraz opis kompletnej polityki bezpieczeństwa wykorzystywanej w systemie AraMIS, tj. obejmującej wszystkie kolejne etapy działania systemu: od monitorowania zagrożeń do reagowania na nie.

3. Czy Autor rozwiązał postawiony problem i czy użył do tego celu właściwych metod?

Osiągnięcia opisane w rozprawie doktorskiej mgra inż. Wojciecha Niewolskiego skłaniają do wyciągnięcia wniosku, że Doktorant rozwiązał postawiony problem realizacji systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych, jak i przyjętej polityki bezpieczeństwa oraz, że wykazał tym samym tezę rozprawy dotyczącą możliwości zbudowania takiego systemu. Istotnie, na podstawie wyników rozprawy, można uznać, że zaprojektowany system AraMIS jest w stanie realizować zadanie dynamicznej adaptacji poziomu bezpieczeństwa adekwatnie do potrzeb oferowanych usług.

Zawartość rozdziałów rozprawy, w tym w szczególności rozdziałów 4-6 pokazuje, że Doktorant zastosował w celu rozwiązania postawionego problemu właściwe metody. Zarówno stopień złożoności problemu analizowanego w rozprawie, jak i mechanizmy wykorzystane w celu jego rozwiązania (w tym np. bazujące wykorzystaniu architektury sieci neuronowej do detekcji anomalii) należy uznać za adekwatne w odniesieniu do typowych wymagań stawianym rozprawom doktorskim.

Oprócz ocenianej rozprawy, na uwagę zasługują także:

1) publikacje Doktoranta, w tym cztery artykuły opublikowane w czasopismach ujętych jako pozycje [49], [123], [271], [272] wykazu literatury rozprawy:
   - IEEE Access (jedna praca) - obecnie 100 pkt MEiN z roku 2021,
   - Electronics, MDPI (dwie prace z 2021 r. i z 2022 r.) – obecnie 140 pkt MEiN,
   - Journal of Network and Computer Applications, Elsevier z 2023 r. – obecnie 140 pkt MEiN (praca mająca status "w recenzji" w rozprawie, lecz niedawno opublikowana),

   które mogą być uznane za powiązane z tematyką rozprawy doktorskiej,
2) wartości parametrów naukometrycznych, w tym w szczególności liczby cytowań prac Autora wynoszącej 59 (według Google Scholar) na dzień finalizacji niniejszej recenzji, które podkreślają rangę wyników badań Doktoranta w środowisku międzynarodowym.

Na podkreślenie zasługuje także wysoce praktyczny charakter osiągnięć Doktoranta, który wynika nie tylko z wdrożeniowego charakteru doktoratu przygotowanego w ścisłym związku z firmą Orange. Jest on widoczny również poprzez udział Doktoranta w dwóch projektach („Access control in 5G MEC" oraz "INSPIRE-5Gplus"), jak i szereg raportów wewnętrznych Orange współautorstwa Doktoranta, których sześć jest ujętych w wykazie literatury ocenianej rozprawy jako pozycje [121], [124]-[127] oraz [252].

Oceniana rozprawa doktorska charakteryzuje się ponadto poprawną strukturą, a jej treść została starannie opracowana i sformatowana. W mojej ocenie wykaz literatury obejmujący obszerny zestaw 276 pozycji ukazuje stan sztuki w sposób adekwatny do charakterystyki poruszanego tematu rozprawy.

4. Jakie są słabsze strony rozprawy?

Oceniana rozprawa doktorska jest moim zdaniem wysokiej jakości i pozbawiona istotnych wad. Moje uwagi są następujące:

1. Pomimo ogólnie bardzo dobrego stylu prezentacji wyników pracy, w pracy można zauważyć w kilku miejscach pewne kwestie stylistyczne/literowe, np.
   - str. 13: „... ze zwiększona potrzebą mocy obliczeniowych" → „...z potrzebą zwiększenia mocy obliczeniowej" lub „...z potrzebą zwiększonej mocy obliczeniowej"
   - str. 14: „...jest ona bardziej skompilowana..." → „...jest ona bardziej skomplikowana..."
   - str. 20: „Nie mniej" → „Niemniej"

2. Rysunki w rozprawie zostały ogólnie przygotowane w sposób staranny i szczegółowy. Jednakże, w przypadku kilu z nich należałoby rozważyć zwiększenie ich rozmiaru (np. rys 3.3, 3.4), gdyż tekst zawarty w nich jest słabo czytelny. Ogólnie zdecydowanie lepszym rozwiązaniem istotnie podnoszącym czytelność rysunków rozprawy byłoby wstawienie ich do rozprawy w formie grafiki wektorowej, a nie punktowej.

3. Doktorant analizując właściwości projektowanego systemu, bazuje na typowym cyklu obejmującym sekwencję etapów identyfikacji, ochrony, detekcji, reakcji i działań naprawczych, który klasycznie jest dedykowany reagowaniu na indywidualne zagrożenia. W tym kontekście warto byłoby rozszerzyć analizę o weryfikację skuteczności projektowanego systemu w scenariuszach:

   a) równoległego występowania zagrożeń (mogących wpływać na siebie wzajemnie, w tym w szczególności zwiększać rozmiar negatywnych konsekwencji),

   b) ataków przeprowadzanych w okresie, kiedy sieć nie ma pełnej zdolności operacyjnej (np. w okresie awarii masowej kilku jej elementów uwarunkowanej np. działaniem sił natury – pożarem, silnymi opadami deszczu, itp.).

Powyższe uwagi mają charakter uwag drobnych bądź polemicznych i nie rzutują na moją sumaryczną pozytywną ocenę rozprawy.

5. Do której z następujących kategorii Recenzent zalicza rozprawę:

a/ nie spełniająca wymagań,
b/ wymagająca wprowadzenia poprawek i ponownego recenzowania,
c/ zadowalająco spełniająca wymagania,
d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem),
e/ wybitna?

Moja sumaryczna ocena rozprawy doktorskiej mgra inż. Wojeciecha Niewolskiego jest **pozytywna**. Wynika ona przede wszystkim z istotnych osiągnięć Doktoranta zawartych w rozdziałach 4-6 rozprawy, jak i starannego przygotowania samej rozprawy. Z uwagi na spełnione moim zdaniem ustawowe wymagania, **wnoszę o dopuszczenie rozprawy doktorskiej mgra inż. Wojciecha Niewolskiego do publicznej obrony**.

Ponadto, ranga osiągnięć Doktoranta ukazanych w rozprawie poparta opublikowaniem przez Doktoranta szeregu prac w rozpoznawalnych czasopismach (które wymieniam w sekcji 3 niniejszej recenzji) sprawia, że niniejszą rozprawę zaliczam do kategorii:

d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem).

Z powyższych powodów, **wnoszę o rozpatrzenie możliwości wyróżnienia rozprawy.**

Jacek Rak

AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Wydział Informatyki, Elektroniki i Telekomunikacji

INSTYTUT TELEKOMUNIKACJI

Dr hab. inż. Piotr CHOŁDA

Kraków, dn. 11 sierpnia 2023 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych
Autor rozprawy: mgr inż. Wojciech Niewolski

1. WSTĘP

Praca została zrealizowana w ramach programu „Doktorat wdrożeniowy" pod opieką promotora pana prof. dr. hab. inż. Zbigniewa Kotulskiego z Politechniki Warszawskiej. Wyniki przedstawiono w formie liczącej 260 stron napisanej w języku polskim rozprawy doktorskiej, zawierającej co następuje: Streszczenie (str. 3), streszczenie w języku angielskim Abstract (str. 4), Spis treści (str. 5-6), Rozdział 1 zawierający tezę „Cel i zakres pracy" (str. 7-11), Rozdział 2 „Wprowadzenie" (str. 12-38), Rozdział 3 „Analiza zagrożeń i systemów bezpieczeństwa występujących w obecnych rozwiązaniach obliczeniowych" (str. 39-79), Rozdział 4 „Proponowany system adaptacji bezpieczeństwa" (str. 80-139), Rozdział 5 „Badanie skuteczności systemu adaptacji bezpieczeństwa AraMIS" (str. 140-173), Rozdział 6 „Metody usprawnienia procesu orkiestracji w środowiskach brzegowych" (str. 174-214), Rozdział 7 zawierający także opis publikacji i wystąpień Doktoranta „Podsumowanie badań i wnioski" (str. 215-224), licząca 276 pozycji Bibliografia (str. 223-248), Wykaz używanych skrótów (str. 249-252), Spis tabel (str. 253), Spis rysunków (str. 254-256), Załącznik 1 „Cechy uwzględnione do detekcji w systemie AraMIS" (str. 257-258), Załącznik 2 „Typy sieci neuronowych" (str. 259), Załącznik 3 „API do tworzenia detektorów" (str. 260).

2. CEL BADAŃ (W ODNIESIENIU DO TEZY ROZPRAWY). Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?

Praca dotyczy zagadnień bezpieczeństwa nowoczesnych systemów teleinformatycznych, co w pełni uzasadnia zgłoszenie jej w ramach dyscypliny Informatyka Techniczna i Telekomunikacja. Doktorant postawił sobie za cel opracowanie systemu zapewniającego bezpieczeństwo dla usług rozproszonego przetwarzania danych w oparciu o podejście wielochmurowe, przy czym system ma się automatycznie dopasowywać do różnego rodzaju zmiennych warunków (jak poziom bezpieczeństwa, typ zagrożenia, charakter świadczonych usług, polityka

Akademia Górniczo-Hutnicza | Wydział Informatyki, Elektroniki i Telekomunikacji
Instytut Telekomunikacji
al. A. Mickiewicza 30, 30-059 Kraków,
tel. +48 12 617 39 37, fax +48 12 634 23 72
e-mail: kt@agh.edu.pl, www.agh.edu.pl

ochrony itp.). System został nazwany AraMIS (Adapted 5G+ MultiCloud Intelligent System). Został wytworzony w firmie, w której realizowano doktorat wdrożeniowy, tj. Orange. Samo zajęcie się tematyką świadczenia usług bezpiecznych w nowoczesnej infrastrukturze teleinformatycznej jest jak najbardziej cenne i oznacza potrzebę zmierzenia się z nietrywialnymi problemami. Wykonanie założonego systemu, który nie tylko zarządza bezpieczeństwem, ale dodatkowo samodzielnie się adaptuje, to duże osiągnięcie i jak najbardziej pożądany wynik doktoratu w ramach nauk inżynieryjno-technicznych.

Cele pracy Doktorant przedstawił w podrozdziale 1.2 „Teza pracy", przy czym ten tytuł jest nieco mylący, gdyż żadnej tezy w zasadzie nie postawiono (samo w sobie nie jest to, moim zdaniem, wadą). Za to Autor czytelnie przedstawia cele pracy, czyli „pokazanie możliwości zbudowania systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych" (str. 8). Tak ***zdefiniowany cel jest czytelny, prawidłowo określony i pożądany.*** W praktyce Doktorant realizuje go z pomocą szeregu pomniejszych zadań, zdefiniowanych na str. 8-9, spośród których jako najważniejsze należy wskazać opracowanie systemu monitoringu, mechanizmu opisu bezpieczeństwa oraz jego wymuszania. Wszystko to służy zabezpieczeniu opartych na technice 5G systemów MEC (tj. systemów obsługi obliczeń typu chmurowego na brzegu sieci). Jest to aktualne zagadnienie techniczne o dużej istotności dla teleinformatyki.

3. SPOSÓB PRZEPROWADZENIA ANALIZY ŹRÓDEŁ. SPOSÓB SFORMUŁOWANIA WNIOSKÓW WYNIKAJĄCYCH Z ANALIZY ŹRÓDEŁ. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Niestety Doktorant nie zdecydował się na przedstawienie odrębnego rozdziału analizującego stan wiedzy oraz źródła literaturowe, co zdecydowanie byłoby przydatne, gdyż pozwalałoby czytelnie przedstawić inspiracje, nawiązania, przeciwstawić swoje wyniki cudzym osiągnięciom, wskazać braki wypełnione przez dokonania własne itd. Nie można jednak powiedzieć, żeby te aspekty nie znalazły się w rozprawie, gdyż analiza literaturowa jest obecna, tyle że rozproszona i niekonsekwentna (w dużym stopniu jest ujęta w rozdz. 2-3, ale zdarza się również w innych miejscach, np. podrozdz. 4.1.1, o tym piszę zresztą niżej). Nie mam wątpliwości, że ***Doktorant posiada odpowiednią (i to bardzo szeroką) wiedzę, zarówno teoretyczną jak i praktyczną, w zakresie tematyki objętej rozprawą.***

Rozdział 2 trafnie przedstawia stan techniki w odniesieniu do konglomeratów koncepcji stojących za grupą technik tworzących 5G (przede wszystkim z punktu widzenia płaszczyzny sterowania) oraz za podejściami charakterystycznymi dla MEC, jak również związanymi z nimi problemami integracji. Pokazano również, jak przedstawione koncepcje łączą się z resztą pracy. Model MEC adekwatny do pracy został oparty na popularnym i powszechnie uznawanym podejściu standaryzowanym przez organizację ETSI.

Rozdział 3 to przegląd stanu techniki (ale też rozwiązań otwartoźródłowych i komercyjnych) odnoszących się do podatności systemów na ataki. Doktorant przeanalizował różne podatności i zagrożenia, jak również sposoby przeciwdziałania

im. Zwrócił również uwagę na narzędzia oraz na kwestię ich adaptowalności (podkreślając słusznie, że ten aspekt nie jest na razie zadowalająco zrealizowany; jest to istotne gdyż faktycznie w podjęciu się realizacji tego rodzaju właściwości można upatrywać dużej oryginalności doktoratu). Prezentacja w zasadzie jest pełna, ale bardzo niekonsekwentna. Np. materiał przedstawiony w tabeli 3.1 jest wprawdzie wyczerpujący, ale trudno uznać go za dobrze sklasyfikowany. Po pierwsze, niektóre ze wskazanych zagrożeń są niejasno rozdzielone (np. w kategorii „Outages" podane przypadki raczej nie są rozłączne; niejasne jest też rozdzielenie zagrożeń w kategorii katastrof). Po drugie, sposób opisu bywa nawet zagadkowy dla czytelnika, ale nie wiem, czy w sposób zamierzony (np. w przypadku DDoS i ataku polegającego na podszywaniu się Autor podaje te same trzy obszary wpływu, ale w innej kolejności – czy to ma na coś konkretnego wskazywać?). Ponadto w niektórych przypadkach Doktorant wskazuje na ocenę wpływu danego zagrożenia, a w innych tego nie robi. Niektóre sposoby kwalifikacji wydają się sporne (np. zaliczenie wycieku danych do uszkodzenia). Niekonsekwentne jest też użycie pojęcia ryzyka: czasem Doktorant mówi o nim w formie mnogiej (co raczej wskazuje na utożsamienie z pojęciem zagrożenia czy ataku), a czasem jako o pewnym parametrze mierzalnym tylko w liczbie pojedynczej (jak w definicji ze str. 50, chociaż w niej w zasadzie pominięto kwantyfikację prawdopodobieństwa zajścia zdarzenia, zwracając uwagę tylko na wpływ). Przy spostrzeżeniu tych wad należy też jednak zwrócić uwagę, że Doktorant dużo bardziej interesująco i trafnie opisuje zagadnienia mu bliskie – np. specyficzne zagrożenia dla środowisk MEC w podrozdz. 3.4 (w ogóle prace własne Doktoranta są opisane dużo lepiej w drugiej części pracy, poczynając od rozdz. 4; ale i tam zdarzają się fragmenty dotyczące opisu stanu techniki). Szczególnie wartościowa jest analiza istniejących rozwiązań, przy czym Doktorant trafnie rozgranicza, jakiego rodzaju adaptacja systemów jest proponowana w odniesieniu do bezpieczeństwa. Jednakże w tabeli 3.6 ponownie niekonsekwentnie opisano istniejące rozwiązania (czasem mówi się o konstrukcji oprogramowania, czasem o zapewnianych funkcjach, niekiedy o narzędziach wizualizacji – chyba w każdym opisywanym przypadku trzeba byłoby powiedzieć o tym wszystkim). Poza tym, zamiast opisu werbalnego (lub jako jego uzupełnienie), można było już w tej części pracy rozważyć po prostu rozbicie pożądanych funkcjonalności w taki sposób, żeby odnosić się do nich zero-jedynkowo (są lub ich nie ma), co też umożliwiłoby zestawienie ich z rozwiązaniem opracowanym przez Doktoranta. W zasadzie takie zestawienie jest dokonane, ale na bardzo późnym etapie pracy, co z punktu widzenia strukturalnego nieco zaburza odbiór. Doktorant dokonuje tego dopiero w podrozdz. 5.4, co ma znaczenie niejako podsumowujące rezultaty, podczas gdy oczekiwałoby się takiego zestawienia raczej jako podsumowania analizy zastanego stanu techniki – wtedy przekonująco uzasadniałoby ono określone decyzje odnoszące się do projektowanego systemu.

Analiza stanu wiedzy/techniki jest rozsiana również w innych fragmentach pracy, także w dużo głębiej wchodzących w prezentację wyników własnych Doktoranta. Dotyczy to np. zestawienia narzędzi do wykrywania incydentów w środowiskach teleinformatycznych (podrozdz. 4.2.1). Skądinąd te zestawienia wskazują na świetne zorientowanie Autora rozprawy w obszarze praktyki współczesnego bezpieczeństwa. Zestawienia zostały dokonane również po to, żeby zdecydować, które z narzędzi zewnętrznych można zintegrować z opracowywanym systemem, ewentualnie jakie braki w istniejących narzędziach należy uzupełnić w rozwiązaniu AraMIS. Z tego punktu widzenia jasne są inspiracje oraz powody, dla których

Doktorant zdecydował się zrealizować różne elementy funkcjonalne. Potem nawet w podrozdziale 6.1 znajduje się charakterystyka narzędzi do opisu polityk bezpieczeństwa, zaś w 6.3 przegląd interpreterów do realizacji niskopoziomowej polityki bezpieczeństwa.

W zakresie opisu stanu wiedzy na temat uczenia maszynowego, w ramach którego Doktorant zresztą w zasadzie nie prowadzi badań (ale które wykorzystuje bardzo twórczo i jako istotny wkład w projektowany system) można wskazać pewne wady szczególnie związane z opisem w podrozdz. 4.2.1. Po pierwsze, rys. 4.9 użyty jako podsumowanie klasyfikacji jest niezbyt szczęśliwy: co najmniej brakuje na nim wskazania sztucznych sieci neuronowych w odniesienia do zastosowań klasyfikacyjnych (a przecież w takim właśnie sposób używa ich sam Autor), nie występuję na nim również regresja logistyczna (którą potem Autor charakteryzuje). Po drugie, opisy modeli są nieprecyzyjne lub nawet nietrafne, np. w odniesieniu do naiwnego klasyfikatora Bayesa (który zresztą jest nazywany po angielsku i to raczej kolokwialnie „Naive Bayes") naiwność jest tłumaczona w sposób „To złożenie upraszcza obliczenia i dlatego jest uważane za naiwne": otóż prawdą jest, że chodzi o uproszczenie obliczeń, ale przecież nie dlatego mówi się o naiwności, ale ze względu na to, o czym Doktorant napisał zdanie wcześniej, tj. ze względu na niezależność występowania różnych cech. Z kolei opis lasów losowych wprawdzie mówi o aspekcie losowości w odniesieniu do używanych w poszczególnych klasyfikatorach składowych próbkach danych, ale nie wspomina, że różne klasyfikatory wykorzystują również losowo wybrane cechy. Szerszy przegląd różnych architektur sztucznych sieci neuronowych Doktorant zawarł w podrozdz. 4.2.3. W ramach przeglądu Autor zwraca uwagę na dostosowanie wybranych architektur (wykorzystuje potem niektóre z nich do wykrywania i klasyfikacji zagrożeń) do zadań, do których zamierza ich używać w projektowanym systemie. Również w tym przypadku Doktorant nie ustrzegł się pewnych uproszczeń i braków (np. nie wspomina, że jednak warstwy LSTM to rozszerzenie RNN, zaś przedstawiając te ostatnie w zasadzie wcale nie wyjaśnia, dlaczego dobrze nadają się do zastosowań: „Ten typ sieci neuronowej dobrze nadaje się do wykrywania anomalii, ponieważ może wykrywać wzorce w danych, które nie są zgodne z oczekiwanym zachowaniem" – w zasadzie opis ten ma charakter tautologiczny i pasuje do wszelkich modeli wykrywających elementy odstające; potem prawie taki sam opis jest podany w przypadku architektur GAN, które przecież działają inaczej niż RNN). Zwracam uwagę na te potknięcia opisu, bo trudno o nich nie wspomnieć, ale myślę że one wynikają raczej z nieprzyłożenia się do dokładnego scharakteryzowania wiedzy zastanej niż z czego innego.

Bibliografia obejmuje 276 pozycji, z których wprawdzie nie wszystkie to pozycje naukowe (jest np. wiele odnośników do oprogramowania), ale jako całość bez wątpienia odniesienie do tekstów dowodzi zorientowania we współczesnym stanie badań oraz – przede wszystkim – stanie techniki związanych z tematyką pracy. Nie ma wątpliwości, że ***dziedzina jest świetnie opanowana przez Doktoranta, który ma na czym budować własne propozycje rozwiązań***.

4. **ROZWIĄZANIE PRZEDSTAWIONEGO ZADANIA, WŁAŚCIWOŚCI PRZYJĘTYCH METOD I ZAŁOŻEŃ. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione? ORYGINALNOŚĆ ROZPRAWY, SAMODZIELNY DOROBEK AUTORA, POZYCJA ROZPRAWY W STOSUNKU DO STANU WIEDZY (POZIOM TECHNIKI) PREZENTOWANEGO W LITERATURZE ŚWIATOWEJ. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?**

Rozprawa ma w zasadzie charakter konstrukcyjny, gdyż Doktorant przedstawia system, który opracował i wdrożył na potrzeby jednego z operatorów. Według deklaracji Doktoranta opracowany system AraMIS łączy funkcjonalności obecnie najbardziej zaawansowanych koncepcyjnie typów systemów zabezpieczania SOAR (security orchestration automation and response) oraz XDR (extended detection and response), z czym się zgadzam – przy czym za najbardziej nowatorski od strony naukowej aspekt uważam związany ze sposobem wykrywania zagrożeń. W ogólności ***Doktorant poprawnie zrealizował cel pracy***, co pisuję poniżej. Najbardziej oryginalne rozdziały pracy to 4-6; przedstawiono w nich sam system AraMIS, w którym zgodnie z deklaracją Doktoranta każdy wyróżniony element składowy jest adaptowalny z punktu widzenia uruchomionego procesu bezpieczeństwa.

Rozdział 4 przedstawia moduł służący do monitorowania zagrożeń. Jest on skonstruowany modułowo, pozwalając na odrębne potraktowanie podsystemu monitoringu zagrożeń, jak i reagowania na nie. Doktorant zwraca uwagę, że przynajmniej niektóre z elementów składowych systemu były tworzone w sposób zapewniający energooszczędne działanie. Podsystem wykrywania zagrożeń używa dużego zestawu cech (maksymalnie 240, chociaż występuje też wersja oparta na mniejszej ich liczbie), które zasilają modele uczenia maszynowego różnego rodzaju. Do wyboru cech Doktorant używa kilku wskaźników, chociaż nie jest do końca sprecyzowane, jakie właściwie to wskaźniki (jak się wydaje są to entropia Shannona czy wartość Shapleya, ewentualnie pewne dane pochodzące z metody XGBoost), ale nie zostały one jasno opisane. Faktem jest, że metody oparte na tego rodzaju wskaźnikach są z powodzeniem stosowane do wyboru cech na potrzeby analizy danych w uczeniu maszynowym. Doktorant przebadał również, jak dobrze wybrane cechy sprawdzają się w wykrywaniu czterech reprezentatywnych zagrożeń. Takie postępowanie również się stosuje i jest to podejście metodologicznie poprawne. W ogólności zmniejszenie liczby używanych cech i ich dobór jest trafnie udokumentowane, a z punktu widzenia badawczego można ten aspekt uznać za jeden z najciekawszych i najbardziej twórczych w rozprawie. Ponadto Doktorant przedstawia inne opisane ilościowo rezultaty związane z doborem modeli uczenia maszynowego. Wprawdzie samo uczenie maszynowe jest tutaj potraktowane narzędziowo i nie zawsze podano pełny proces dochodzenia do uzyskania zadowalających modeli (pominięto głównie cały aspekt metodologiczny związany ze strojeniem hiperparametrów, a w niektórych przypadkach w ogóle nie podano szczegółów, np. nt. wartości parametru k w przypadku metody k najbliższych sąsiadów, wskaźnika czystości w przypadku drzew decyzyjnych czy typu funkcji jądrowej w przypadku metody wektorów nośnych).

Inny niezwykle wartościowy aspekt pracy to opisany w podrozdz. 4.2. projekt dotyczący detekcji zagrożeń, który ma na celu oszczędzanie zasobów, które dodatkowo skwantyfikowano w kategoriach zmniejszania zużycia energii. Aspekt ten

jest również powiązany z kluczowym nowatorskim elementem opracowywanego systemu, tj. jego adaptowaniem się. W tym przypadku sprawa dotyczy automatycznego doboru narzędzi do wykrywania zagrożeń na podstawie reguł decyzyjnych, które uruchamiają bardziej złożone modele dopiero gdy prostsze modele wskazują, że może to być zasadne; jest to tzw. dynamiczna aktywacja modeli (inny aspekt adaptowalności systemu polega dodatkowo na tym, że interfejs systemu pozwala dołączać kolejne modele uczenia maszynowego). Doktorant bierze pod uwagę głównie wielkość modelu, ale też sposób ich reprezentacji i przetwarzania (serializacja). Modele wykrywania podejrzanego zachowania są najpierw oparte na klasyfikacji zero-jedynkowej (w ogólności wykrywanie zachowań anomalnych), a potem ewentualnie stosuje się model klasyfikacji wielopoziomowej. Najbardziej zaawansowane modele wykrywania zachowań anomalnych opierają się na użyciu zaawansowanych architektur autokoderów (także wariacyjnych z elementem generatywnym).

Doceniam zwrócenie uwagi na aspekt oszczędności energii, chociaż trzeba powiedzieć, że Doktorant nie podaje tutaj pomiarów z systemu rzeczywistego, a raczej szacuje oszczędności pośrednio, tj. używa raportowanych w literaturze ilości dotyczących zmniejszenia użycia energii przy np. redukcji pamięci itd. Bardzo ciekawe byłoby zbadanie, jakie faktycznie zmniejszenie jest uzyskiwane w praktyce. To jednak raczej postulat niż krytyka wyników.

Rozdział 5 pokazuje, w jaki sposób zachowuje się opracowany system w środowisku, w którym przeprowadzono zgodnie z wybranymi scenariuszami kilka typów ataków. W tym celu Doktorant skonstruował środowisko eksperymentalne, w którym łączy elementy technik 4G i 5G, realizując elementy w oparciu o adekwatne techniki wirtualizacji. Od strony praktycznej system zasługuje na uwagę, gdyż opracowanie tego rodzaju rozbudowanego i realistycznego środowiska eksperymentalnego nie jest trywialne, ponadto wyniki uzyskane w taki sposób (a nie np. na podstawie symulacji) istotnie zyskują na jakości, gdyż są bardziej przekonujące. Wybrane cztery scenariusze zagrożeń/ataków są reprezentatywne. W przypadku każdego z nich obserwacje były prowadzone przez kilka godzin, badania były też powtarzane (inna sprawa, że Doktorant nie poświęca zbyt wiele miejsca reprodukowalności wyników czy ich analizie z punktu widzenia wiarygodności statystycznej). To w tym rozdziale Doktorant pokazuje rezultaty uzyskane z badań wspomnianych modeli wykrywania anomalii, a potem z klasyfikacji służącej rozróżnianiu różnych typów ataków (one z kolei zostały oparte na kilku płytkich modelach uczenia maszynowego). Wyniki są opisane w sposób standardowy dla zadań klasyfikacji, tj. z użyciem wskaźników opartych na macierzy pomyłek (w przypadku klasyfikacji zero-jedynkowej, bo niestety dla klasyfikacji wielostanowej pokazano po prostu całe macierze bez informacji nt. liczebności przedstawicieli poszczególnych klas), a w przypadku modyfikacji progów wykrycia anomalii dla tego samego klasyfikatora – na podstawie charakterystyki ROC. Wyniki są poprawnie interpretowane, a uzyskane wartości wskazują, że system z tego punktu widzenia może być bardzo użyteczny. To również w tym rozdziale Doktorant dokładniej opisuje adaptację systemu z punktu widzenia różnych aspektów wykrywania zagrożeń. Przedstawiono trzy modele, które w ogólności rozróżnia się na podstawie efektywności detekcji, ewentualnie unikania błędów pierwszego lub drugiego rodzaju. Doktorant zestawia trzy opracowane modele optymalizacji doboru modeli wnioskowania nie tylko z punktu widzenia uzyskiwanych przez nie wskaźników dokładności, precyzji i NVP (użyte zasadniczo adekwatnie, chociaż zaskakuje brak oparcia się wprost na wskaźniku czułości), ale także z punktu

widzenia wspomnianej wcześniej oszczędności zasobów. Przedstawione przez Doktoranta wyniki tego rodzaju uważam za szczególnie interesujące, tym bardziej że dyskutuje, do których ewentualnie technologii mogłoby mieć one zastosowanie w praktyce. Uważam, że tego rodzaju wyniki są też najciekawsze jako najlepiej umotywowane i skwantyfikowane z punktu widzenia naukowego.

Rozdział 6 referuje zagadnienia zarządzania systemem AraMIS jako całością, także w aspekcie integracji różnych elementów (też zewnętrznych), ale przede wszystkim tzw. orkiestracji z naciskiem na bezpieczeństwo. Elementy składowe są wspomagane przez narzędzia zewnętrzne, z jednej strony m.in. z grupy obejmowanej przez Elastic, tj. popularny system zarządzania danymi pozyskiwanymi z sieci, a z drugiej strony przez rozwiązanie NodeRED. Integrowane są też inne popularne narzędzia (np. snort). To jest aspekt ważny od strony wdrożeniowej, chociaż niekoniecznie badawczej, ale na pewno podnosi wartość praktyczną opracowanego systemu jako całości. Ponadto system jest wyposażony we własny interfejs graficzny. W ramach rozdz. 6 Doktorant charakteryzuje sposób definiowania wymogów bezpieczeństwa oraz realizacji polityk bezpieczeństwa w środowisku MEC współpracującym z 5G. Doktorant przedstawia rozszerzenie swojego systemu w oparciu o opis grafowy polityki bezpieczeństwa. Dodatkowo prezentuje elementy modułu MEC Enabler, który służy do zaimplementowania funkcji bezpieczeństwa z użyciem funkcji sieciowych modelu płaszczyzny sterowania 5GC. Również ten element zapewnia adaptowalność systemu (w tym przypadku dotyczy ona dostosowania do potrzeb związanych z wymaganym poziomem bezpieczeństwa). W zakresie zarządzania bezpieczeństwem przedstawione szczegóły rozwiązania od strony inżynierskiej są istotne, chociaż trudno się do nich w szczegółach odnieść ze względu na fakt, że Doktorant nie przedstawia ich działania w sposób ujmowany kwantyfikowalnie ani w taki sposób, który dawałby szansę na porównanie z innymi systemami. Nie jest też jasne, czy elementy zarządcze systemu można byłoby skonstruować inaczej, gdyż Autor nie rozważa głębiej ewentualnych alternatyw koncepcyjnych. Niemniej jednak jako całość system bez wątpienia działa i jego konstrukcja stanowi istotne osiągnięcie praktyczne.

Kilka drobnych wątpliwości merytorycznych, wynikających być może tylko z opisu:

- Doktorant zajmuje się adaptacją bezpieczeństwa, ale nie wprowadza miary, która służyłaby do kwantyfikacji poziomu tej adaptacji, co byłoby pożądane w celu oszacowania, na ile się ona udaje, na ile można jej poziom porównać z innymi rozwiązaniami itd.
- Jedna z metod doboru cech używanych do opisu danych wejściowych dla modeli uczenia maszynowego jest w podrozdz. 4.1.3 scharakteryzowana w sposób sugerujący jakoby oparto się na twierdzeniu Shannona (str. 94), tymczasem z podpisu osi na rys. 4.4 wynika, że po prostu chodzi o entropię. Nie wiadomo, które twierdzenie Shannona Doktorant ma na myśli i czy nie jest to pomieszanie twierdzenia z wielkością (tj. z entropią Shannona).
- Doktorant charakteryzuje jeden z modułów systemu AraMIS, który po angielsku nazywa się „Hyper parameters Tuning", raczej w sposób sugerujący przygotowanie danych do zadania klasyfikacji z użyciem uczenia maszynowego (np. normalizacja danych). W ogóle nie wspomina jednak w ramach opisu o odpowiedniku polskim angielskiej nazwy, tj. strojeniu hiperparametrów, co dotyczy doboru możliwości działania samego modelu uczenia maszynowego. Nawiasem mówiąc, polskie

tłumaczenie nazwy modułu („Moduł selekcji i oceny parametrów") jest o tyle nietrafne, że hiperparametr i parametr modelu uczenia maszynowego to zupełnie co innego (parametry podlegają procesowi uczenia, podczas gdy hiperparametry są dobierane w innego rodzaju procedurze metaoptymalizacyjnej). W ogóle bardzo ważna z punktu widzenia uczenia maszynowego kwestia doboru hiperparametrów jest wielkim nieobecny tej pracy doktorskiej. Wierzę, że w czasie publicznej obrony będzie możliwość dyskusji od strony metodologicznej tego obszaru prac.

Podsumowując, nie mam wątpliwości, że ***rozprawa przedstawia oryginalne i wartościowe rozwiązanie realnego zagadnienia z obszaru teleinformatyki, które zostało uzyskane z użyciem poprawnie zastosowanych metod***. Warto też zwrócić uwagę, iż Doktorant oparł rozprawę na szeregu współtworzonych przez siebie dokumentów, w tym dziewięciu artykułów naukowych oraz szeregu dokumentów wewnętrznych firmy. Na uwagę zasługuje, że z jednej strony wyniki zostały wdrożone w firmie Orange, a z drugiej strony fakt że część cytowanych artykułów powstała z udziałem autorów spoza Polski (także w ramach projektu międzynarodowego).

5. **POPRAWNOŚĆ PRZEDSTAWIENIA UZYSKANYCH WYNIKÓW. Czy Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?**

Praca jest napisana w sposób czytelny. Zasadnicze koncepcje są dobrze zrozumiałe. Niektóre elementy strukturalne są niepotrzebnie rozwinięte (np. szczegóły interfejsu graficznego, które od strony badawczej raczej nie wnoszą nic istotnego), a także wymieszane (tj. prezentacja stanu wiedzy/techniki z rozwiązaniami oryginalnymi Doktoranta). Nie zaburza to jednak istotnie odbioru treści.

Od strony redakcyjnej praca jest akceptowalna, ale zawiera niestety dużo wad. W zakresie potknięć dotyczących przedstawiania wyników muszę wskazać:

- Użycie pewnych terminów w sposób niejednolity, np. mam wrażenie, że pojęcie „slice" jest używane jako zasoby typu slice, sieci plastrowe (oba na str. 23) oraz fragment sieci (str. 24). Tutaj jest tylko kwestia niejednolitego tłumaczenia, ale we wcześniej wspomnianym przypadku rozumienia ryzyka (piszę o tym wyżej w punkcie 3 niniejszej recenzji) mamy do czynienia z różnymi pojęciami.
- Potknięcia strukturalne: np. drzewa decyzyjne są wprowadzone z punktu widzenia modelowania na str. 113, ale Autor uprzednio prezentuje pewne wyniki uzyskane dzięki nim na str. 97. Na pewno nie sprzyja to płynności czytania.
- W przypadku niektórych rysunków należałoby zwiększyć ich rozmiar, bo są nie do końca czytelne, np. w przypadku rys. 3.3 liternictwo w ogóle jest małe, a napisy w lewym dolnym rogu są praktycznie nie do odczytania (podobnie w tab. 6.1). Dotyczy to też ważnych rysunków z wynikami własnymi Autora (np. zamieszczone w tab. 4.5 czy 4.8, także rys. 4.10).

- Niekonsekwencje w prezentacji materiału z użyciem języka angielskiego (a praca jednak została napisana po polsku): na przykład treść tab. 1.1-1.3, 3.2, 4.7 lub wykaz sektorów gospodarczych na str. 35 (w zasadzie nie ma uzasadnienia brak tłumaczenia na język polski), także materiał na wielu rysunkach (np. 3.1-3.9); niekiedy nietłumaczenie pojęć (np. w tab. 3.4, chociaż skądinąd duża część materiału jest podana w języku polskim). Niektóre modele uczenia maszynowego, które Doktorant nazywa tylko po angielsku, mają swoje uznane odpowiedniki (np. drzewa decyzyjne czy lasy losowe).
- Użycie języka polskiego:
    - Problemy z interpunkcją – przecinki zdecydowanie są nadużywane i często stawiane w nielogicznych miejscach (np. „Analiza opisanych powyżej serwisów, wykazała potrzebę..." na str. 3 czy też „Zazwyczaj, proponowana ochrona usług" na str. 7 – tutaj być może Doktorant zanglicyzował zasady polskiej interpunkcji; w ogólności ten problem jest nagminny i zdarza się prawie na każdej stronie, gdzie występuje więcej tekstu), chociaż trzeba powiedzieć, że niekiedy przecinki nie pojawiają się tam, gdzie akurat mogłyby być przydatne (np. „należy upewnić się jak jej egzekwowanie może..." na str. 177; chociaż to ma miejsce o wiele rzadziej). Nadmierne użycie interpunkcji naprawdę utrudnia czytanie, bo zmusza umysł do przetwarzania niepotrzebnego znaku przestankowego i generalnie jest irytujący.
    - Zdarzają się przypadki występowania nieporadnego lub nawet błędnego stylu, np. „Do zalet wymienionego rozwiązania można wymienić..." na str. 14, „dane dowodzą na to..." na str. 40, „którą wielokrotnie wysyła lub opóźniania" na str. 47 czy „Wizualizacja pełen cyklu" w tytule rys. 3.5).
    - Użycie nie w pełni adekwatnych słów czy pojęć (np. „prędkość" zamiast „szybkość" w odniesieniu do łącza na str. 18), kolokwializmów (np. „rozszywających" w odniesieniu do tuneli GTP-U na str. 21) lub anglicyzmów (np. „na bazie" zamiast „na podstawie" w tytule rys. 1.2 na str. 20, „procent" zamiast „odsetek" w tytule rys. 3.2, ewentualnie użycie zestawienia ze słowem „dla" zamiast „odnoszący się do" czy tp. w tym samym tytule), stwierdzenie że incydent może być „zaradzony" (na str. 50), odnoszenie czasownika „posiadać" do rzeczownika, którego desygnatem nie jest osoby czy instytucja (np. w odniesieniu do rozwiązań na str. 53); na str. 62 użyto fatalnego z punktu widzenia technicznego kolokwializmu „mniej optymalne".
    - Niegramatyczne tłumaczenie fraz, które nie stanowią problemu w języku angielskim ze względu na brak deklinacji, ale rażą w języku polskim ze względu na niezgodność przypadków (np. „serwis odpowiedzialny za przydzielanie oraz zarządzanie zwirtualizowanymi zasobami" zamiast „serwis odpowiedzialny za przydzielanie zwirtualizowanych zasobów oraz zarządzanie nimi" na str. 27).
    - Błąd ortograficzny polegający na rozdzielnym zapisaniu spójnika „nie mniej" na str. 35 i 62.

- Niewyrównanie dużych fragmentów tekstu: bibliografii oraz wypunktowań.
- Niedopasowanie opisów do zamieszczonych rysunków, np. na stronie 23 są opisane funkcje sieciowe 5GC, których nie ma na rys. 1.3 (np. NSSF).
- W rozdziale 2 numeracja rysunków i tabel zaczyna się niekonsekwentnie (tj. np. rys 1.1 zamiast 2.1 itd.).
- Niekiedy występujące literówki (głównie pogubione litery lub krótkie przyimki albo odstępy), np. „Fog Computig" na str. 13, „anomali" na str. 57, „zawiera się przedziale" na str. 51, „wraz wykrywaniem" na str. 74, „przedstawione załączniku nr1" na str. 93, „reprezentację entropi" czy „Wskaźnik entropi" na str. 94, „Decission Tree" na str. 96. Zdarza się pisownia nazwiska matematyka od małej litery, jak w „bayes" na str. 243.
- Niekonsekwentna konwencja stosowania kolorów, przez co przedstawiane wyniki mogą mylić i są trudniejsze w interpretacji (tak jest w przypadku rys. 4.7 i 4.8: w jednym kolor niebieski oznacza „data leak", podczas gdy na drugim rysunku ten kolor oznacza „normal", który z kolei na pierwszym jest reprezentowany z użyciem koloru zielonego).
- Opis bibliograficzny:
  - Autor zdecydował się na kolejność związaną z cytowaniem (co często praktykuje się w przypadku publikacji konferencyjnych lub w periodykach naukowych), a nie w kolejności charakterystycznej dla prac quasi-monograficznych jak rozprawa doktorska;
  - niektóre pozycje literaturowe nie są w pełni opisane i niekiedy nie wiadomo, co to w ogóle za teksty (np. [7], [8], [15], [19], [52], [60], [149], [152]);
  - niekonsekwentny opis literatury w zakresie podawania skróconej lub pełnej wersji imion autorów (por. np. różnica między opisem [48] i [49]), ewentualnie podawania wolumenów i numerów lub nie (np. [97]), czasem używane są wersaliki do opisu nazwisk, niekiedy tytuły prac są podawane z cudzysłowami.

Myślę, że co najmniej niektórych ze wskazanych wad redakcyjnych dało się uniknąć przy nieco bardziej starannej redakcji rozprawy.

6. SŁABE STRONY ROZPRAWY, JEJ GŁÓWNE WADY. Jakie są słabe strony rozprawy i jej główne wady?

Nie widzę istotnych wad rozprawy. Omówione już wcześniej kwestie:

- brak wydzielonego rozdziału na analizę literaturową, co łączy się również z wymieszaniem strukturalnym prezentacji wyników oryginalnych z opisem i analizą wiedzy zastanej;
- niekonsekwentny opis stanu wiedzy i techniki (np. różne sposoby rozumienia ryzyka, wątpliwe klasyfikowanie zagrożeń itd.);
- potknięcia językowe, szczególnie interpunkcyjne, jak również redakcyjne

nie stanowią w moim przekonaniu istotnego obciążenia dla jakości pracy jako całości. Przede wszystkim nie mam zarzutów odnośnie do realizacji od strony merytorycznej.

7. PRZYDATNOŚĆ ROZPRAWY DLA NAUK TECHNICZNYCH, PRZEMYSŁU, OBRONNOŚCI KRAJU ITP.

Rozprawa przedstawia wyniki, które powstały jako realizacja systemu na potrzeby operatora telekomunikacyjnego i bez wątpienia w odpowiedzi na jego autentyczne potrzeby. W związku z tym, że system dotyczy jak najbardziej aktualnej techniki (5G) oraz zastosowań (MEC) ***przydatność pracy dla przemysłu jest oczywista***. Część z prowadzonych badań jest ***interesująca z punktu widzenia nauk inżynieryjno-technicznych*** (tj. Informatyki Technicznej i Telekomunikacji). W tym przypadku należy wskazać przede wszystkim dobór cech potrzebnych do automatycznego wnioskowania nt. zagrożeń we współczesnych systemach teleinformatycznych, jak również wypracowanie koncepcji adaptowalnego z punktu widzenia używanych zasobów (w tym: energii) sposobu konstrukcji potoku modeli uczenia maszynowego służących do klasyfikacji zagrożeń.

8. PODSUMOWANIE (CZY ROZPRAWA SPEŁNIA WYMAGANIA PRZEZ OBOWIĄZUJĄCE PRZEPISY) ORAZ OCENA ROZPRAWY. Do której z następujących kategorii Recenzent zalicza rozprawę (niepotrzebne skreślić)?

Doktorant wykazał wiedzę i umiejętności w zakresie tworzenia współczesnych systemów zabezpieczających infrastruktury 5G/MEC, które są obsługiwane przez narzędzia analizy danych opartej na uczeniu maszynowym. Na podstawie tej wiedzy był w stanie skonstruować bardzo rozległy i oryginalny system, który ma zastosowania u operatora telekomunikacyjnego. Z tych powodów stwierdzam, że ***rozprawa spełnia aktualne wymagania dotyczące prac doktorskich i wnioskuję o dopuszczenie jej do obrony***.

W zakresie oceny rozprawy jako całości kwalifikuję ją jako:

~~a. Nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy~~

~~b. Wymagająca wprowadzenia poprawek i ponownego recenzowania.~~

~~c. Spełniająca wymagania.~~

d. Spełniająca wymagania z wyraźnym nadmiarem.

~~e. Wybitnie dobra, zasługująca na wyróżnienie.~~

Piotr Chołda