Prof. dr hab. inż. Janusz Kacprzyk, członek rzecz. PAN
Fellow of IEEE (Life), IET, EurAI, IFIP, IFSA, SMIA
Instutut Badań Systemowych
Polskiej Akademii Nauk
Ul. Newelska 6
01-447 Warszawa
Email: kacprzyk@ibspan.waw.pl

Warszawa, 12 czerwca 2023

Recenzja rozprawy doktorskiej mgr. inż. Jarosława Homy pt. „Implementacja algorytmów synchronizacji urządzeń sieciowych bazujących na paradygmacie programowalnych sieci komputerowych"

Niniejsza recenzja została przygotowana w odpowiedzi na prośbę p. prof. dr hab. inż. Andrzeja Polańskiego, Przewodniczącego Rady Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Śląskiej w Gliwicach, wyrażoną w stosownym piśmie.

Rozprawa dotyczy najogólniej pewnych oryginalnych rozwiązań sprzętowych i programowych dla cyberbezpieczeństwa, które od pewnego czasu staje się jednym z największych wyzwań współczesnego świata mającym wpływ na wszelkie aspekty życia, zarówno ekonomiczne, jak społeczne, dotyczące bezpieczeństwa i wszelkie inne, przy czym ma to wpływ zarówno na jednostki ludzkie, grupy społeczne, jak też różnego rodzaju firmy, organizacje, instytucje itp. działające we wszystkich dziedzinach.

Mówiąc bardziej konkretnie, rozprawa poświęcona jest zaproponowaniu oryginalnych i efektywnych implementacji algorytmów synchronizacji urządzeń sieciowych dla środowiska programowalnych sieci komputerowych SDN (ang. software designed networks) mających za zadanie wykrywanie i mitygację ataków sieciowych z rodziny rozproszonych odmów obsługi, czyli tzw. DDoS (ang. distributed denial of service). W pracy proponuje się nowoczesne i obiecujące rozwiązanie polegające na zaprojektowaniu i implementacji wspomnianego systemu w środowisku sieciowym SDN z centralnym kontrolerem i wspomagającymi go modułami decyzyjnymi. Co jest ważne i stanowi na pewno o nowoczesności i oryginalności propozycje Doktoranta, to szerokie użycie elementów sztucznej inteligencji, a przede wszystkim uczenia maszynowego, w szczególności głębokiego uczenia. Jest to zgodne

z najnowszymi trendami w tej dziedzinie. Ponadto, zaproponowany system zawiera moduły z zaimplementowanymi algorytmami wykrywania ataków i mitygacji ich skutków, jest skalowalny, a do tego kwestie jego niezawodności i bezpieczeństwa zostały szeroko i efektywnie uwzględnione.

Jako tezę pracy przyjęto: „Możliwe jest opracowanie systemu mitygacji ataków sieciowych, opartego o rozwiązanie programowalnych sieci komputerowych SDN, wykorzystującego nowatorskie algorytmy sterowania i synchronizacji urządzeń, w tym analizę uzyskaną za pomocą algorytmów sztucznej inteligencji". Jest to niewątpliwie teza dotycząca ważnego zagadnienia i ambitnych rozwiązań.

Zatem, można stwierdzić, że praca dotyczy bardzo ważnych zagadnień, stanowiących wyzwanie i naukowe i praktyczne, a przyjęte w niej główne założenia i zaproponowane rozwiązania odpowiadają obecnemu stanowi wiedzy i bez wątpienia reprezentują nowoczesne rozwiązania. To, co podsumowano powyżej, zostało zawarte w Rozdziale 1 „Wstęp", który jest bardzo dobrze napisany.

W tym miejscu wydaje się, że należy poczynić następującą uwagę. Otóż ta praca ma niewątpliwy charakter wdrożeniowy, co jest trudne w informatyce w systemie polskim, ponieważ np. nie jest możliwe patentowanie rozwiązań informatycznych, nawet bardzo oryginalnych, jak to jest w wielu innych krajach. Na szczęście, w niniejszej pracy jest też wiele elementów charakterystycznych dla tradycyjnych doktoratów typu teoretycznego, czyli elementów nowości zarówno w zakresie architektury systemu i jego modułów oraz algorytmów i ich implementacji.

W dalszej części recenzji omówię i ocenię dokładniej zaproponowane rozwiązania, przy czym omówię według kolejności rozdziałów, co ułatwi sprawę, ponieważ przyjęta w pracy chronologia kolejno opracowywanych rozwiązań, a tez ich opisu w kolejnych rozdziałach, jest uzasadniona i efektywnie prowadzi do rozwiązania zamierzonego celu.

W Rozdziale 2 „Przegląd literatury" zawarto przede wszystkim krytyczna ocenę różnych rozwiązań stosowanych do realizacji rozpatrywanych w pracy klas zagadnień, odnosząc je do głównej literatury przedmiotu, co jest wyborem dobrym i cennym, dając od razu obraz

głównych kierunków badań, implementacji i wdrożeń oraz pozwalając od razu docenić to, że rozwiązanie w pracy jest zgodne i nowoczesnymi tendencjami, a do tego oryginalne.

Na początku Doktorant przedstawia główne rodzaje cyberataków zakłócających sieci komputerowe. Omawia jako główne zagrożenie rozproszone ataki odmowy usługi (DDoS) i wskazuje, że szczególnie są tym dotknięte wieloskalowe sieci komputerowe, których bezpieczeństwo jest krytyczne, a jednocześnie silnie zagrożone ze względu na lawinowy wzrost liczby cyberataków. Wymaga to efektywnych i skalowalnych rozwiązań.

Autor następnie słusznie koncentruje się na atakach typu rozproszonych odmów obsługi (DDoS – ang. distributed denial of service), także ich wielowektorowej wersji, zwłaszcza opartych na zalewie protokołów, co ma na celu wyczerpanie zasobów obliczeniowych atakowanego hosta, głownie jego procesora, pamięci i pasma sieciowego.

Doktorant pokazuje różne metody walki z atakami DDoS, zarówno w sensie propozycji naukowych, jak implementacji, a nawet wdrożeń, oraz wskazuje na niedostatecznie szerokie ich wdrożenie do powszechnego użycia ze względu na duże wymagania sprzętowe, pamięciowe itp.

Autor omawia też różne koncepcje systemu wykrywania włamań IDS (ang. intrusion detection system), niewątpliwie jednego z najważniejszych elementów bezpieczeństwa sieci. Dobrze byłoby w tym miejscu omówić np. relacje między DDoS i IDS, bo to nie jest jasna i tu i w dalszych rozdziałach.

W następnej, bardzo ważnej części tego przeglądu literatury, implementacji i wdrożeń, Autor celnie wskazuje na wielki potencjał programowalnych sieci komputerowych SDN (ang. software defined networks), które pojawiły się stosunkowo niedawno jako nowa koncepcja i zyskały sobie już popularność, ponieważ jest w nich oddzielona płaszczyzna sterowania siecią od płaszczyzny danych, a także zakłada się programowalności samego sterownika. Autor analizuje krytycznie zalety tego paradygmatu i zakłada go w proponowanych przez siebie rozwiązaniach.

Następnie, Autor rozpatruje ważny problem bezpieczeństwa sieci SDN, a zwłaszcza różne podejścia do jego zapewnienia, przy czym szczególną uwagę poświęca nowoczesnym

rozwiązaniom opartym na uczeniu maszynowym, w szczególności na głębokim uczeniu (ang. deep learnng).

Ten krótki, ale bardzo dobrze zrobiony przez Autora przegląd literatury i rozwiązań w zakresie głównej tematyki rozprawy jest ważny dla pracy, bo bardzo dobrze uzasadnia późniejsze wybory Autora dotyczące systemu informatycznego mitygacji ataków DDoS opartego o paradygmat sieci SDN, w zakresie zarówno architektury i algorytmiki proponowanego systemu, a także jego implementacji, co zrealizowano potem w rozprawie.

Część poświęcona sieciom komputerowym SDN jest bardzo ważna. Autor przedstawia, ale też uzasadnia potrzebę i możliwość użycia w dalszej części pracy wielu elementów, które dotyczą może nie tylko sieci SDN, ale innych narzędzi algorytmicznych i technicznych, które są ogólniejsze, ale tu są stosowane w systemie zrealizowanym z użyciem paradygmatu SDN.

Na początku, podaje się w bardzo jasny i poglądowy sposób koncepcję programowalnych sieci komputerowych SDN (ang. software defined networks), która pojawiła się dopiero w 2007 r. i szybko zyskała popularność wśród teoretyków i praktyków. Istotną rolę odegrał tu protokół OpenFlow, na którym koncepcja SDN jest oparta.

Autor celnie wskazuje na to, że ważne dla jego rozwiązań jest tu rozdzielenie płaszczyzn sterowania (ang. control plane) i płaszczyzny danych (ang. data plane) oraz zastosowanie kontrolera, który jest odpowiedzialny za działanie wszystkich urządzeń sieciowych SDN w płaszczyźnie danych, Jest to dobre rozwiązanie ogólnie i cenne dla pracy, bo np. może obniżyć koszt modyfikacji konfiguracji. Architektura sieci SDN zawiera przy tym 4 warstwy: przekazywania danych, kontrolną, aplikacji i zarządzania siecią, Jest to dobra architektura, a do tego umożliwia wgląd we wszystkie anomalne sytuacje występujące w sieci, które są na bieżąco rejestrowane przez kontroler. Dobrze byłoby tu wyjaśnić, dlaczego wcześniej i np. na rys 2 pokazuje się architekturę trójwarstwową, co może skłaniać czytelnika do przekonania, że taka właśnie architektura jest typowa czy nawet jedyna, a w opisie mówi się już o architekturze czterowarstwowej. Tak jest zresztą i w innych miejscach pracy. Dobrze byłoby to wyjasnić.

Oczywiście, programowalność pozwala na implementacje różnych modułów i jest kluczowa. Pozwala także na bezpośrednio, programowalne sterowanie siecią, m.in. optymalizację zasobów sieciowych, użycie automatyzacji programów, zdefiniowanych na otwartych standardach itd. OpenFlow jest tu stosowanym protokołem, a kluczowe elementy dla SDN to: przełącznik OpenFlow (vSwitch), kontroler OpenFlow (SDN Kontroler) i protokół OpenFlow. W rozwiązaniach będących wynikiem rozprawy nacisk jest położony na implementacje kontrolerów SDN w wersjach z otwartym kodem (ang. open source), oczywiście wspierających protokół OpenFlow. Kontrolery SDN udostępniane są przy tym jako pakiety instalacyjne dla odpowiednich systemów operacyjnych.

W dalszej części niniejszego rozdziału Autor dokładnie omawia szczegóły architektur i implementacji tych elementów charakterystycznych dla systemów opartych na użyciu paradygmatu SDN, Oprócz bardzo dobrego przeglądu literatury ma to duże znaczenie dla pracy, ponieważ te omawiane rozwiązania techniczne, ich cechy i trudności związane z ich implementacją jasno pokażą w późniejszych rozdziałach oryginalność zaproponowanych w pracy rozwiązań.

Przy omawianiu tego rozdziału pracy należy wspomnieć, że Autor zawarł tu krótki przegląd probabilistycznych i statystycznych metod teorii informacji, głównie opartych na pojęciu entropii. W dalszej części pracy jest to stosowane do analizy anomalii w sieciach opartych na paradygmacie SDN. Jest to ciekawe i dobre rozwiązanie, zgodne zresztą z rolą, jaką metody oparte na entropii odgrywają w wielu analizach różnych systemów, w tym systemów informatycznych. Podobnie, pokazano użycię popularnych reguł typu IF—THEN do wykrywania włamań.

Szczególną rolę odgrywa tu pkt. 2.2.3 poświęcony przedstawieniu zastosowań uczenia maszynowego do klasyfikowania ruchu w sieciach i wykrywania anomalii, przy czym pokazano zastosowanie uczenia nadzorowanego, trenowanego przez dane z ruchu, a więc bez możliwości wykrywania nieznanych sygnatur, oraz nienadzorowanego, poprzez np. grupowanie danych w oparciu o podobieństwo niektórych cech, umożliwiające wykrywanie nieznanych sygnatur. Jest to bardzo dobry przegląd literatury, choć może brakuje uwag na temat np. które z wyników uzyskanych w literaturze, w sensie metod uczenia maszynowego, są najbardziej właściwe dla rozpatrywanych zadań.

W pracy stosuje się właśnie metody uczenia maszynowego, co jest niewątpliwie pewną nowością, choć może należy podkreślić, że ważniejsze i pewno bardziej perspektywiczne może tu być zastosowanie metod tzw. głębokiego uczenia DL (ang.deep learning), które zyskało wielka popularność w ostatnich czasach. Uważam, ze dobrze byłoby zamieścić w pracy więcej informacji zarówno na temat samego głębokiego uczenia (głębokich sieci neuronowych), jego zastosowań w dziedzinie pracy, a także implementacji tych nowoczesnych podejść, zwłaszcza w dziedzinie ogólnie rozumianego cyberbezpieczeństwa.

Podsumowując, moja ocena tego rozdziału jest bardzo pozytywna. Autor przedstawił bardzo dobry, obszerny, ale i krytyczny, przegląd nowoczesnych rozwiązań związanych z rozpatrywanymi w pracy różnymi aspektami systemu i jego funkcjonalnościami. Te rozwiązania wyraźnie wskazują na to, jak ten projektowany system powinien być zaprojektowany i zaimplementowany, co będzie przedmiotem dalszych rozdziałów.

Rozdział 3 „Proponowane rozwiązanie problemu" to już podstawowa część pracy, która w sposób jawny korzysta z doskonałego przeglądu literatury i rozwiązań praktycznych dotyczących ogólnie rozwiązań systemów mitygacji ataków sieciowych DDoS z użyciem sieci komputerowych SDN, ale też analizy metod i algorytmów wykrywania ataków zarówno z użyciem bardziej tradycyjnych metod, jak też nowoczesnych metod uczenia maszynowego, zwłaszcza uczenia głębokiego. W wyniku tej analizy Autor trafnie zaproponował, aby ten system był modułowy, skalarny i działający w sposób rozproszony w sieci Internet. Zostało to zaprojektowane, a potem zaimplementowane, w postaci systemu STRAINER.

Ogólnie, system STRAINER ma na celu: wykrywanie dwóch podstawowych grupy ataków sieciowych z rodziny DDoS: wolumetrycznych i aplikacyjnych, działa w oparciu o paradygmat sieci komputerowych SDN, a detekcja anomalii jest głównie skupiona w kontrolerze sieci SDN z niezbędnymi modułami i systemami dodatkowymi. Koncepcja systemu zostanie przedstawiona w dalszej części pracy, system jest modułowy z autorską i nowatorską architekturą, projektem i implementacją poszczególnych modułów. System zbudowano przy tym, uwzględniając pełną redundancję, skalowalność i elastyczność implementacji itp.

Jeżeli chodzi o wdrożenie powyższego systemu, co ma kluczowe znaczenie dla niniejszej pracy, to jest ono realizowane poprzez wariantowe scenariusze wdrożenia, co jest bez wątpienia dobrym rozwiązaniem.

Tak więc, bez wątpienia system STRAINER, który jest wynikiem pracy, jest niewątpliwie oryginalnym rozwiązaniem, zarówno w sensie projektowym, algorytmicznym, jak też implementacyjnym i wdrożeniowym.

W dalszej części rozdziału Autor rozwija i wyjaśnia wiele aspektów związanych z powyższymi rozwiązaniami, funkcjonalnościami itp. realizowanymi przez system. Najważniejsze i najciekawsze z nich to chyba wyjaśnienie na wstępie różnic między odmową obsługi (DoS – ang. denial of service) a rozproszona odmowa usługi (DDoS – ang. distribute denial of service), atakami wolumetrycznymi poprzez wysyłanie pakietów z rozproszonych hostów typu „zombi" oraz atakami aplikacyjnymi nakierowanymi na konkretna aplikację internetową, najczęściej rozproszoną, w celu całkowitego wyczerpania zasobów systemowych hosta aplikacji, np. pamięci. Bardzo dobry jest też przegląd metod i systemów ochrony przed atakami DDoS, przede wszystkim w aspekcie mechanizmów prewencyjnych i reaktywnych.

System STRAINER jest przedstawiony w sposób konstruktywny, m.in. przez analizę rozwiązań, które pozwoliłyby zrealizować pożądane funkcjonalności, Jest to bez wątpienia osiągnięcie Autora, zarówno w sensie nowatorskiej koncepcji, architektury, jak też implementacji i koncepcji wdrożenia. Mówiąc bardziej konkretnie, preferowanym obszarem działania systemu STRAINER jest obszar mechanizmów reaktywnych wykrywania ataków ze względu na wszystkie zaklasyfikowane sposoby detekcji, a także do pewnego stopnia reakcja na atak.

W dalszej części rozdziału przedstawia się w podobny, konstruktywny i kompleksowy sposób system mitygacji ataków DDoS biorąc pod uwagę to, że system STRAINER dysponuje trzema reaktywnymi modułami detekcji anomalii sieciowych w sensie ataków DDoS.

Pierwszy moduł, MOD1, charakteryzuje się bardzo szybkim działaniem detekcyjnym i jest oparty o „lekkie" algorytmy wykrywania anomalii na podstawi bazy znanych sygnatur. Natomiast, drugi moduł, MOD2, jest oparty o algorytmy detekcji anomalii poprzez użycie

metod uczenia maszynowego, w szczególności metodę lasów losowych (ang. random forest) Breimana, a moduł trzeci, MOD3, poprzez użycie głębokiego uczenia.

W pacy pokazuje się zarówno zamierzone funkcjonalności tych modułów, ich projektowanie, stosowane algorytmy, jak też ich implementacje i uwagi o ich wdrożeniu. Ogólnie, są to oryginalne rozwiązania Autora z punktu widzenia wszystkich aspektów, czyli funkcjonalności, architektury, projektu, algorytmów i implementacji. Oprócz niewątpliwej oryginalności z punktu widzenia tych aspektów, bardzo ciekawe jest uwzględnienie przez Autora wymagań co do wydajności systemu poprzez propozycję pewnych modyfikacji dla różnych założonych poziomów planowanej wydajności. Trzeba też podkreślić, że użycie metod uczenia maszynowego, a szczególnie głębokiego uczenia, jest rozwiązaniem bardzo nowoczesnym i obiecującym. Także przykładem dobrego rozwiązania jest użycie reguł typu IF—THEN. To samo można też powiedzieć o zastosowaniu metod teorii informacji opartych na entropii. Jednocześnie, może dobrze byłoby nieco więcej miejsca poświęcić użyciu tych metod uczenia maszynowego, w szczególności głębokiego uczenia, zwłaszcza głębokich sieci neuronowych, bo to najprawdopodobniej będzie coraz bardziej popularne i w literaturze i w rozwiązaniach praktycznych..

Bardzo ciekawym fragmentem pracy jest pokazanie kilku scenariuszy możliwego wdrożenia systemu. Nie mam wątpliwości, że jest to oryginalne osiągnięcie Autora, bardzo ważne dla niniejsze pracy typu doktoratu wdrożeniowego. W tym miejscu można też wspomnieć o autorskiej propozycji rozproszonego systemu ochrony przed atakami DDoS opartego na użyciu sieci SDN z przetwarzaniem brzegowym (ang. edge computing), co może mieć znaczenie dla przyszłych rozwiązań w tej dziedzinie.

W dalszej części rozdziału przedstawiono bardzo wyczerpujący, ale jednocześnie zrozumiały, wykaz wszystkich praktycznie elementów sytemu STRAINER będącego przedmiotem pracy. Zamieszczono dokładny opis najpierw architektury oraz implementacji algorytmów, np. synchronizacji urządzeń sieciowych, a także wzorcowe zbiory danych dla potrzeb stosowanych algorytmów uczenia maszynowego, itp. Opis modułów systemu STRAINER jest też bardzo ciekawy i dobrze pokazuje możliwości systemu, przy czym podkreślić trzeba, że te moduły zawierają autorskie i innowacyjne rozwiązania w sensie architektury, algorytmów i ich implementacjo oraz procedur wdrażania. Moja opinia o tej części pracy jest także bardzo pozytywna.

Rozdział 4 „Opis środowiska testowego, testy weryfikacyjne sytemu" zawiera bardzo dobre przedstawienie wyników pracy, przy czym w tym rozdziale dotyczy to działania systemu STRAINER, i zbadania wydajności, dokładności i szybkości jego działania. Dla tej fazy prac zbudowano środowisko testowe zawierające zarówno sprzęt jak i oprogramowanie. Jako oprogramowanie przyjęto: Mininet 2.3.0 – wirtualne środowisko sieciowe, zawierające wirtualne urządzenia sieciowe (vSwitch) i interfejsy do sieci rzeczywistej, które jest kluczowym elementem zaprojektowanego systemu służącym do emulacji sieci. Instancje kontrolerów SDN są w formie maszyn wirtualnych lub zintegrowanych w Mininet. System pracuje pod kontrolą systemu operacyjnego Linux Debian, a użyto skryptowego Python z odpowiednimi bibliotekami. Sprzętowo, środowisko sieciowe zwierało siedem przełączników Open vSwitch, 45 hostów oraz 10 serwerów, a było uruchomione na czteroprocesorowym serwerze (Intel Xeon Gold 6230) wyposażonym w 2 TB pamięci RAM. Do symulacji ataków zastosowano znane i uznane oprogramowania, przede wszystkim Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution i LOIC – Low Orbit ION Cannon network stress testing application.

Nie mam tu uwag krytycznych, zarówno strona sprzętowa jak związana z oprogramowaniem są właściwe i odpowiadają nowoczesnym rozwiązaniom w tym względzie.

W dalszej części rozdziału zawarto wyniki bardzo rozbudowanych różnego rodzaju testów dla poszczególnych modułów systemu, do których oceny zastosowano znane i efektywne wskaźniki, głównie: liczbę poprawnych klasyfikacji ataku przyjętą jako wynik prawdziwie dodatni (ang. True Positive, TP), liczbę poprawnych klasyfikacji ruchu normalnego przyjętą jako wynik prawdziwie ujemny (ang. True Negative, TN), liczbę niepoprawnych klasyfikacji ataku jako ruchu normalnego przyjętą jako wynik fałszywie ujemny (ang. False Negative, FN), liczbę niepoprawnych klasyfikacji ruchu normalnego jako ataku przyjętą jako wynik fałszywie dodatni (ang. False Positive, FP), a skuteczność detekcji (dokładność wykrycia) przyjętą jako: sumę wartości powyższych wskaźników. Jest to dobre rozwiązanie, a użycie true/false positive/negative, co jest często stosowane do analizy wielu krytycznych systemów i zadań, daje dodatkowy wgląd w uzyskane wyniki.

W powyższym środowisku testowym przeanalizowano różne sytuacje dla poszczególnych modułów, przede wszystkim różne typy ataków DDoS, konkretnie dziewięć różnych żądań.

Pokrywają one chyba dość dobrze to, co zdarza się w praktyce, choć może celowe byłoby wyjaśnienie, czy np. te żądania są najważniejsze, czy najczęściej się zdarzają itp. Otrzymane wyniki są ciekawe i wartościowe, a – co jest ważne – są dobrze udokumentowane i przedstawionoew sposób jasny i poglądowy, ponieważ już nawet np. opisy, czy nawet tekst w nagłówkach tabel, jest zrozumiały.

W dalsze części rozdziału rozpatrzono podobne testy, ale już dla sytuacji, gdy zaprojektowany i zaimplementowany system pracuje w tzw. systemie produkcyjnym, co jest niezwykle ważne w przypadku niniejszej pracy o charakterze wdrożeniowym. Najogólniej biorąc, działanie systemu w systemie produkcyjnym nie odbiegało znacząco od jego działania w trybie testowym. Jest to niewątpliwie duże osiągnięcie Autora.

Podsumowanie

Podsumowując moją opinię na temat pracy, pragnę stwierdzić, że:

- Praca dotyczy bardzo ważnego wyzwania stojącego przed światem, a mianowicie ogólnie rozumianego cyberbezpieczeństwa, w szczególności jednego z najważniejszych problemów w powyższej dziedzinie, czyli mitygacji ataków DDoS,
- Autor przyjął do realizacji powyższego celu nowoczesne rozwiązania typu sieci SDN, użycie metod sztucznej inteligencji, w szczególności uczenia maszynowego, zwłaszcza głębokiego uczenia,
- Autor zastosował do testowania, a potem implementacji i wdrożenia systemu właściwe środki algorytmiczne, programowe i sprzętowe,
- Autor wykazał się bardzo dobra znajomością literatury przedmiotu oraz nowoczesnych rozwiązań technicznych, co właściwie ukierunkowało Jego prace,
- Praca jest kompletna w sensie użycia właściwych środków sprzętowych i programowych zarówno w fazie projektowania i implementacji, jak i potem wdrażania.

Moja ocena jest przy tym szczególnie pozytywna, ponieważ w tym doktoracie wdrożeniowym są także zawarte wyraźne elementy nowości i innowacyjnych rozwiązań, co jest raczej cechą charakterystyczną zwykłych doktoratów typu badawczego. To

połączenie „nauki" i „praktyki" jest, jak wspomniałem na początku, szczególnie trudne w przypadku systemów informatycznych, ale Autor sobie z tym bardzo dobrze poradził.

W związku z powyższym, stwierdzam, że – moi zdaniem – **rozprawa spełnia wszelkie wymagania ustawowe i zwyczajowo przyjęte w polskim środowisku naukowym** stawiane rozprawom doktorskim i wnoszę o jej **przyjęcie oraz dopuszczenie do publicznej obrony**.

Jednocześnie, ze względu na wspomniane już zalety pracy, proponowałbym, żeby w przypadku odpowiedniego przebiegu obrony i innych etapów postępowania, rozpatrzyć jej **wyróżnienie**, zgodnie z zasadami obowiązującymi w Politechnice Śląskiej.

J. Kopyl