Gdańsk, 15 listopada 2021

Dr hab. inż. Rafał Leszczyna
Politechnika Gdańska
Wydział Zarządzania i Ekonomii
rle@zie.pg.edu.pl

Recenzja rozprawy doktorskiej

mgr inż. Grzegorza Siewruka

pt. „Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego"

Promotor dr hab. inż. Wojciech Mazurczyk, Politechnika Warszawska

Promotor pomocniczy dr inż. Adrian Marzecki

1. Wprowadzenie

Niniejsza recenzja rozprawy doktorskiej, której Autorem jest mgr inż. Grzegorz Siewruk, została wykonana w oparciu o uchwałę Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej (Uchwała nr 181/2021) z dnia 14 września 2021 roku podpisaną przez dr hab. inż. Jarosława Arabasa oraz dr hab. inż. Artura Janickiego. Uchwała ta wskazuje mnie jako recenzenta w komisji doktorskiej w postępowaniu w sprawie nadania stopnia doktora mgr. inż. Grzegorzowi Siewrukowi.

Promotorem niniejszej rozprawy jest dr hab. inż. Wojciech Mazurczyk, profesor Politechniki Warszawskiej. Promotorem pomocniczym jest dr inż. Adrian Marzecki.

2. Podejmowane zagadnienia naukowe

Recenzowana rozprawa doktorska dotyczy zastosowań technik uczenia maszynowego oraz metod przetwarzania języka naturalnego w procesie rozwijania bezpiecznego oprogramowania.

Teza rozprawy oraz jej główne cele zostały przedstawione w rozdziale 1.2. Cele pracy, sformułowane poprawnie oraz spójne z tezą pracy, związane są z (i) eksperymentalną

analizą algorytmów uczenia maszynowego pod kątem możliwości ich zastosowania w procesie wytwarzania bezpiecznego oprogramowania; (ii) zaprojektowaniem i implementacją rozwiązania wspomagającego automatyczne zarządzanie (orkiestrację) narzędzi bezpieczeństwa i proces decyzyjny wdrażania oprogramowania; (iii) wdrożeniem tego rozwiązania; (iv) oraz udowodnieniem jego skuteczności.

3. Zawartość rozprawy

Przedstawiona do recenzji praca zawiera streszczenie, streszczenie w języku angielskim, spis treści, wykaz publikacji, prezentacji i nagród związanych z tematyką rozprawy, listę skrótów, spis tabel, spis rysunków, wprowadzenie, osiem numerowanych rozdziałów, spis pozycji literatury oraz trzy załączniki zawierające instrukcję uruchomienia systemu oraz kopie dyplomów związanych z przedstawionym rozwiązaniem.

Całość rozprawy napisana jest w języku polskim, z wyjątkiem wspomnianego streszczenia w języku angielskim.

Układ i zawartość rozdziałów merytorycznych jest zasadniczo poprawna.

W pierwszym rozdziale (Wprowadzenie) Autor zarysowuje tematykę doktoratu oraz ogólnie przedstawia podjętą problematykę badawczą. Opisane są tutaj też cele i teza rozprawy a także układ pracy.

Rozdziały 2-4 przedstawiają kontekst prowadzonych przez Autora badań, począwszy od obszarów cyberbezpieczeństwa w których wykorzystywane są algorytmy uczenia maszynowego (rozdział 2). W rozdziale trzecim przedstawiono podstawowe modele wytwarzania oprogramowania i problematyce cyberbezpieczeństwa w procesie dostarczania oprogramowania. Natomiast rozdział 4 dedykowany jest wybranym algorytmom uczenia maszynowego oraz technikom przetwarzania języka naturalnego. Poziom szczegółowości opisów nie jest jednorodny. Może zastanawiać dlaczego niektórym zagadnieniom Autor poświęca więcej uwagi, innym mniej a także motywacje stojące za decyzjami dotyczącymi kategorii istniejących rozwiązań. Piszę o tym szerzej w części zatytułowanej „Uwagi dyskusyjne" niniejszej recenzji.

Opis zaproponowanego przez Autora rozwiązania Mixaway oraz związanych z nim badań i eksperymentów rozpoczyna się w rozdziale 5. To tutaj Autor opisuje architekturę Mixaway oraz główne etapy wdrożenia rozwiązania. W rozdziale 6, zatytułowanym „Metodyka badawcza", Autor przedstawia badania eksperymentalne służące do wybrania algorytmu maszynowego do implementacji w rozwiązaniu. Wyniki eksperymentów przedstawiono w rozdziale 7, zatytułowanym „Wyniki badań eksperymentalnych". W tym samym rozdziale znajduje się opis rezultatów uzyskanych dzięki wdrożeniu w rozwiązania.

Bibliografia zawiera 132 pozycje. Są to w przeważającej części artykuły i dokumenty opublikowane w ciągu ostatnich kilku lat. Obok nich znajdują się podstawowe, starsze publikacje z obszarów poruszanych przez Autora. Analiza literatury jest dość szeroka i Autor przedstawia w niej trafne wnioski, co generalnie świadczy o dobrym rozpoznaniu wiedzy w dziedzinie. Pozostałem komentarze dotyczące analizy literatury przedstawiłem w rozdziale „Uwagi dyskusyjne" niniejszej recenzji.

4. Stopień realizacji celów rozprawy

Wszystkie cele rozprawy zostały osiągnięte.

Autor zaproponował system Mixaway wspomagający zarządzanie automatycznymi testami bezpieczeństwa w (wysoce) rozproszonym środowisku wytwarzania oprogramowania, integrującym m.in. zasoby udostępniane w chmurach zewnętrznych. Przeprowadzone badania eksperymentalne pozwoliły Autorowi opracować moduł korelujący wyniki z pomocą technik uczenia maszynowego oraz metod przetwarzania języka naturalnego. Zaprojektowane i zrealizowane rozwiązanie zostało wdrożone w infrastrukturze Orange Polska a o powodzeniu wdrożenia mogą świadczyć uzyskane nagrody przedsiębiorstwa tj. Nagroda szefa funkcji Sieć i Technologie 2019 oraz Security & Privacy Awards 2021. Ponadto system został udostępniony na zasadach licencji otwartego oprogramowania na platformie GitHub skąd pobrano go oraz zainstalowano już ponad 16 000 razy. **Fakty te oceniam bardzo pozytywnie.**

Skuteczność systemu została zweryfikowana eksperymentalnie (analiza modeli uczenia maszynowego w oparciu o zbiór danych pochodzących z infrastruktury rzeczywistego operatora telekomunikacyjnego). oraz na podstawie obserwacji efektów pracy wdrożonego środowiska.

Realizacja celów pracy pozwoliła dowieść jej tezę.

5. Przydatność zaproponowanego rozwiązania w sferze gospodarczej

Zaproponowany przez Autora system Mixaway został wdrożony w sieci operatora telekomunikacyjnego Orange Polska i włączony do procesu dostarczania oprogramowania stu trzydziestu aplikacji. Wpłynęło to na poprawę jakości i skuteczności procesów wytwarzania oprogramowania firmy o czym świadczą wielomiesięczne obserwacje wspieranych przez Mixaway projektów prowadzonych w przedsiębiorstwie. Takie efekty znalazły uznanie w prestiżowych nagrodach przyznanych na poziomie międzynarodowym Grupy Orange oraz przez Orange Polska. Powyższe fakty jednoznacznie potwierdzają wysoką przydatność i praktyczne zastosowanie zaproponowanego rozwiązania w sferze gospodarczej.

Ponadto system jest dostępny na zasadach licencji otwartego oprogramowania na platformie GitHub. Dzięki temu mogą z niego skorzystać także inne przedsiębiorstwa oraz użytkownicy indywidualni. W serwisie GitHub dostępna jest informacja o ponad szesnastu tysięcy pobrań i instalacji oprogramowania Mixeway.

6. Oryginalność rozwiązania

Recenzowana rozprawa doktorska opisuje oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej. W porównaniu z innymi rozwiązaniami opisywanymi w literaturze, system Mixaway, zaproponowany przez Autora, wykorzystuje potencjalne i niepotwierdzone podatności bezpieczeństwa, które zostały zebrane przy pomocy automatycznych skanerów. Ponadto, system posiada możliwość zdalnej kontroli uruchamianych testów podatności co umożliwia automatyzację całego procesu. Ciekawą stroną naukową jest też

wprowadzenie technik uczenia maszynowego do wspomagania decyzji w procesie wytwarzania bezpiecznego oprogramowania.

7. Uwagi dyskusyjne

Autor osiągnął postawione cele rozprawy, udowodnił sformułowaną tezę oraz przeprowadził poprawną ewaluację eksperymentalną. Dołożył też wszelkiej staranności, aby zapewnić poprawność pracy pod względem merytorycznym i redakcyjnym. Poniżej przedstawiam aspekty dyskusyjne, które napotkałem podczas analizy rozprawy.

- Na początku rozdziału 2.1 Autor pisze: „Aplikacje wykorzystujące algorytmy ML w domenie bezpieczeństwa sieciowego mogą być sklasyfikowane do następujących kategorii (na podstawie podziału zaproponowanego w [17]): systemy wykrywania anomalii/włamań oraz ochrona urządzeń końcowych". – Taki podział, na dwie kategorie jest dyskusyjny. Na przykład, jak zgodnie z tą klasyfikacją rozpatrywać fakt, że systemy wykrywania włamań bazujące na detekcji anomalii wykorzystywane są również w ochronie urządzeń końcowych? Poprawności przedstawionej kategoryzacji algorytmów uczenia maszynowego nie wzmacnia fakt, że została ona przedstawiona w artykule ([17]) opublikowanym w serwisie internetowym nie wymagającym recenzji. Jednocześnie należy podkreślić, że główny obszar badań, w którym usytuowana jest praca, czyli orkiestracji narzędzi bezpieczeństwa, został przybliżony w oparciu o rzetelne i wiarygodne źródła wiedzy naukowej ([31]).

- Druga uwaga dotyczy kwestii wyboru przez Autora dwóch spośród pięciu kategorii przedstawionych w artykule [17] bez podania uzasadnienia tego wyboru.

- Zastanawia również dlaczego w części poświęconej rozwiązaniom komercyjnym przedstawiono wyłącznie jedno takie rozwiązanie.

- Z pewnością wartość części pracy związanej z analizą literatury podwyższyłoby przeprowadzenie tego procesu w sposób systematyczny, z wykorzystaniem ugruntowanej metody. W ten sposób zapewnia się gwarancje wysokiej kompletności i uporządkowania. Przykładem systematycznych analiz mogą być te przedstawione w artykułach oznaczonych identyfikatorami DOI: 10.1016/j.compeleceng.2017.11.027 i 10.1016/j.infsof.2013.07.010.

- Nie jest jasne dlaczego rozdział 6 poświęcony opisowi procesu został opatrzony tytułem „Metodyka badawcza", chociaż w treści opisano eksperymenty wykonane przez Autora. W tym środowisko eksperymentalne, wykorzystywane zbiory danych, algorytmy i czynności.

- Również tytuł rozdziału siódmego nie w pełni trafnie oddaje jego treść. Przedstawiono tutaj nie tylko wyniki eksperymentów, ale również praktyczne rezultaty pochodzące z wdrożenia.

- W rozdziale 7.2 nie jest do końca jasne dlaczego Autor najpierw skazuje wartość spadku odrzuceń wdrożenia równą 5% a dalej odwołuje się do wartości 9% omawiając czynniki jakie przyczyniły się do zmniejszenia liczby odrzuceń.

- Także wyjaśnienie w ostatnim akapicie wprowadzenia do rozdziału 7 mające uzasadnić pominięcie dyskusji metryk takich jak odsetek wyników fałszywie negatywnych czy odsetek wyników fałszywie pozytywnych wymagałoby rozszerzenia. W moim odczuciu przedstawienie i omówienie tych metryk stanowiłoby cenną informację w pracy.

Należy zaznaczyć, że wymienione powyżej (w większości drobne) uwagi nie pomniejszają wartości naukowej oraz przydatności i oryginalności rozprawy.

8. Podsumowanie

Przedstawiona do recenzji rozprawa doktorska spełnia ustawowe wymagania stawiane rozprawom doktorskim.

Na tej podstawie wnioskuję o jej dopuszczenie do publicznej obrony w postępowaniu w sprawie nadania stopnia doktora.